CA IT Client Manager

Implementierungshandbuch (Implementation Guide)

12.8

Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden. Diese Dokumentation ist Eigentum von CA und darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden.

Der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, ist berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2013 CA. Alle Rechte vorbehalten. Alle Markenzeichen, Markennamen, Dienstleistungsmarken und Logos, auf die hier verwiesen wird, sind Eigentum der jeweiligen Unternehmen.

CA Technologies-Produktreferenzen

Diese Dokumentation bezieht sich auf die folgenden CA-Produkte:

- CA Advantage® Data Transport® (CA Data Transport)
- CA Asset Intelligence
- CA Asset Portfolio Management (CA APM)
- CA Common Services™
- CA Desktop Migration Manager (CA DMM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Process Automation
- CA Business Intelligence
- CA Service Desk Manager
- CA WorldView™
- CleverPath™ Reporter

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 1: Funktionsweise von CA ITCM 21

DSM-Architektur 21
DSM-Explorer 24
Webkonsole 25
Webkonsolen-Zugriff 25
Funktionen der Webkonsole 25
Unterstützte Web-Browser und Webserver 26
Manager 26
Enterprise- und Domänenkonzept 27
Enterprise- und Domänenkomponenten 28
Die Management-Datenbank im Enterprise- und Domänen-Konzept 29
Engine-Konzept 31
Scalability-Server 38
Unterkomponenten einer Scalability-Server-Basisinstallation 38
Tasks des Scalability-Servers in der Basisinstallation 39
Scalability-Server und Bereitstellung virtueller Anwendungen 40
Aspekte der Boot-Server-Installation des BS-Installationsverwaltung 41
Agent 42
Konzept der Agentenpakete 43
Agentenkonfiguration 44
Remote Control-Viewer 44
Softwarekatalog 45
AM Remote-Agent 46
DSM Reporter 47
Unterstützte Betriebsumgebungen 47
Common Application Framework 48
Benutzeroberfläche des Application Frameworks 48
Taskleiste 49
Protokollierung 50
Allgemeine Konfiguration 52
Konfigurationsparameter 53
Konfigurationsrichtlinien 54
Konfigurationsbericht von Agenten 55
Konfiguration des Enterprise-Manager-Agenten 55
So aktivieren und konfigurieren Sie Standorterkennung 56
Inventarisierung und Verwaltung von Geräten 71
Basisinventar-Komponente 71

Unterstützung für nicht residentes Inventar 72
Beschränkungen von NRI 72

Kapitel 2: Planen der Infrastrukturimplementierung 73

Unterstützung für IPv6 73
Einschränkungen im Kontext der IPv6-Unterstützung 74
Konfigurationshinweise im Kontext der IPv6-Unterstützung 76
FIPS 140-2-Support 80
FIPS 140-2-Plattform-Support 80
Unterstützte FIPS-Modi 81
Failover-Unterstützung und Hardwareersatz 82
Failover-Unterstützung 82
Ersetzen von Managerhardware 85
Konfigurieren von CA HIPS für die Installation von CA ITCM 86
Hinweise zu Komponenten der Infrastruktur 87
Schritte zur Installation der Infrastruktur 88
Schlüsselfaktoren bei der Größenfestlegung der Infrastruktur 88
Computeridentifikation in CA ITCM 89
Roaming von Computern zwischen Domänen 92
Anpassbare Abmeldung oder Neustartbanner 93
Verwenden eines benutzerdefinierten Reboot-Programms 93
Dialogfeld zum Neustarten und Abmelden auf Terminalservern 94
Speicherort der Webdienste-Dokumentation und WSDL-Datei 95
Hinweise zu Webkonsolen und Webservices 95
Interne Abhängigkeiten 99
Abhängigkeiten mit anderen Produkten unter Windows. 100
Manuelle Installation von vorausgesetzten Komponenten unter Windows 103
Abhängigkeiten mit anderen Produkten unter Linux und UNIX 104
Neustarten von Apache unter Linux 104

Kapitel 3: Installation von CA ITCM 105

Funktionsweise des Installationsprozesses 106
Einführung in den Installer 106
Voraussetzungen und Einschränkungen 107
Installationsmethoden 107
Installationshinweise 108
Verschiedene Installationshinweise 109
Installationshinweise zu FIPS 110
Während Installation den FIPS-Modus auswählen 110
Installieren der automatisierten Migration 112
Installationsvoraussetzungen 112

Installationshinweise ... 112
Konfigurieren der automatisierten Migration ... 113
Mehrsprachige Installation ... 113
Informationen zur Erstellung und Installation von Agenten-Sprachpaketen ... 114
Installationsszenarien für bestimmte Agenten ... 115
Erforderliche Hardwarekonfiguration ... 115
Management-Datenbank (MDB) ... 116
MDB-PIF-Paket ... 117
Eigenständige MDB-Installation ... 117
PIF-Installationsdaten ... 118
Hinweise zu CCS ... 118
CCS-Installationsfehlermeldungen ... 119
Vorbedingungen für die DSM-Manager-Installation ... 123
Hinweise zur Festplattenkapazität bei der Installation des DSM-Managers und der MDB ... 123
Eigenständiger Manager in einer gemischten Datenbankumgebung ... 124
Unbeaufsichtigte MDB-Installation mithilfe einer Antwortdatei ... 124
Vorbereitung für das Arbeiten mit einer Microsoft SQL Server-MDB ... 126
Vorbereitung für das Arbeiten mit einer Oracle-MDB ... 129
Hinweise zur Installation und Konfiguration für die Oracle-MDB ... 136
Ändern des Standardkennwortes für den Benutzer "ca_itrm". ... 137
Protokolldateien zur MDB-Installation ... 138
MDB-Upgrades ... 139
Deinstallation ... 140
Besondere Hinweise zu CA ITCM-Installationen ... 140
Einstellungen der Sicherheitsrichtlinie ... 141
Neustart von CAM und SSA PMUX ... 141
Verfügbarkeit des Softwareinventars ... 141
Installation von DSM-Manager mit einer Remote-SQL Server-MDB über IPV6 ... 141
Installation von Domänen-Manager mit Hilfe einer Remote-SQL Server-MDB mit einer benannten Instanz ... 142
Installation des eigenständigen Remote Control-Agenten ... 142
Installation auf Solaris Intel ... 143
Umgebungsvariable PATH für Solaris Intel ... 144
Zugriff auf den VMware-ESX-Webservice ... 144
Installation der Remote Control-Komponente unter Linux ... 145
Installation der Remote Control-Komponente auf Apple Mac OS X ... 145
Freigabezugriff für Boot-Server ... 146
Domänen-Controllerverbindung bei der Installation von CCS ... 146
Verschiebevorgänge der Agent- und Scalability-Server ... 146
DSM-Manager mit CCS WorldView-Manager oder Installation von CCS einschließlich MDB auf einem Domänen-Controller ... 147
Installation eines Scalability-Servers unter Linux ... 148

Installation und Registrierung von UNIX- und Mac OS X-Komponenten 148
Besonderheiten bei UNIX-Agenten 148
Hinweis zur Data Transport Service-Installation 150
Umbenennen von Managern und Scalability-Server-Computern 151
Systemnamen als vollständig qualifizierte Domänennamen 151
Installation von CA ITCM bei vorinstalliertem Unicenter NSM r11 152
Angeben der Port-Nummer für die Webkonsole während der Installation 152
Hinweis zum Hinzufügen der Webkonsole mit Hilfe der Methode zum Ändern der Installation 153
Deaktivieren des Virenschutzes während Installation und Deinstallation 153
Deaktivieren des Remote-Sektorserver-Dienstes während der Installation 153
Windows XP-Netzwerkzugriff - Modell für gemeinsame Verwendung und Sicherheitsmodell für lokale Konten 153
Betrachtungen zu Windows Server 2003 154
Windows Server 2008 Core-Betriebsumgebungen 155
Hinweise zu Firewall und Ports 157
Kompatibilitätsbibliotheken für Linux 157
MSI-Voraussetzungen für den Installer 158
Gemeinsame Verwendung der MDB durch CA Service Desk Manager und CA ITCM 158
Administrative Installation unter Windows 158
Installationsverzeichnisse unter Windows 159
Installationsverzeichnisse unter Linux und UNIX 160
Installieren des Alarm-Collector 161
Einschränkungen für Computer-, Benutzer- und Verzeichnisnamen 162
Einschränkungen für Computernamen 162
Einschränkungen für Benutzernamen 163
Einschränkungen für Verzeichnisnamen 163
Interaktive Installation mit dem Installationsassistenten 164
Prüfung der Festplatte vor der Installation 165
Interaktive Installation einzelner Komponenten 165
Installationszusammenfassung 166
Rollback der Installation 166
Kopie der Installationspakete 166
Hinweise zu CCS 167
Interaktive Installation von CA IT Client Manager unter Windows 167
Interaktive Installation unter Linux und UNIX 169
Installation von CA ITCM über die Befehlszeile in Windows 170
Installationspakete für Windows 170
Installation von CA IT Client Manager mit Hilfe von "setup.exe" 172
Installationstool msiexec 173
Installation von CA ITCM über die Befehlszeile in Linux und UNIX 194
Skript "installdsm" - Installation von CA ITCM unter Linux oder UNIX 195
Einstellung der Antwortdatei unter Linux und UNIX 196

Ändern der Werte der Installationseigenschaften 196
Installationsprotokolldateien 209
Installationsprotokolldateien unter Windows 209
Installationsprotokolldateien unter Linux und UNIX 209
Versionsinformationen zu installierten DSM-Komponenten 210

Kapitel 4: Post-Installationstasks 211

Ändern der Produktsprache nach der Installation 211
Wartung der MDB 212
Microsoft SQL Server-MDB-Wartung 212
Oracle-MDB-Wartung 214
Auf die Ziel-MDB synchronisierte Objekte 215
Deinstallation von DSM-Manager und MDB 219
Installation von SQL Bridge 223
Upgrade der Zielseite mit der Microsoft SQL Server-MDB 1.0.4 224
Upgrade der Zielseite mit der Microsoft SQL Server-MDB 1.5 224
Installation von Oracle Bridge 224
Upgrade der Zielseite mit der Oracle-MDB 1.5 auf Solaris 225
Aktivieren eines Docking-Geräts unter Windows 226
Ausführen der Agenten von der Quelle unter Windows 227
Ausführen von CA ITCM-Diensten über Benutzerkonten unter Windows 228
Ausführen von CA ITCM-Diensten als Administrator 229
Importieren eigener X.509-Zertifikate in das Installations-Image 229
Standardzertifikate für Windows 230
Standardzertifikate für Linux und UNIX 230
Anpassen von X.509-Zertifikaten mit der Datei "cfcert.ini" 231
Ändern und Reparieren einer Installation 233
Ändern einer Installation 234
Reparieren einer Installation: 235
Aktualisierung einer Installation 235
Deinstallation von CA ITCM 236
Deinstallation von CA ITCM unter Windows 237
Deinstallation von CA ITCM unter Linux und UNIX 239
Allgemeine Hinweise zur Deinstallation eines Agenten 240

Kapitel 5: Infrastructure Deployment 243

Einführung in Infrastructure Deployment 244
Typische CA ITCM-Infrastructure Deployment-Phasen 244
Deployment Management-Konzepte 245
Deployment Management-Prozess 249
Bereitstellung über den DSM-Explorer 258

Bereitstellung über die Befehlszeile 259
Von Continuous Discovery ausgelöste Bereitstellung 259
Bereitstellungspakete 260
Das Tool "dsmpush" 262
Voraussetzungen für die automatische Bereitstellung der CA ITCM-Infrastruktur 262
Ändern von FTP-Serverdetails zur Verwendung mit Infrastructure Deployment 266
Windows XP-Einstellung zum Aktivieren der Bereitstellung von Agenten 267

Kapitel 6: Hinweise zu Aktualisierungen und zur Migration 269

Unterstützte Upgrade-Pfade 270
Allgemeine Hinweise 270
Hinweise zum CA ITCM-Komponenten-Upgrade 270
Hinweise zu MDB 271
Hinweise zu Aktualisierungen 271
Upgradeinformationen 272
Hinweise zu FIPS 272
Hinweise zur Aktualisierung für OSIM 273
Aktualisierungsvorgang 274
Wichtige Hinweise zur Aktualisierung 275
Phase 1: Upgrade des DSM-Enterprise-Managers 276
Phase 2: Upgrade des DSM-Domänen-Managers 277
Phase 3: Upgrade der DSM-Scalability-Server 278
Phase 4: Upgrade der DSM-Agenten 279
Upgrade von Agenten mit Hilfe der Installations-DVD 280
Aktualisieren von Windows-Agenten mit Hilfe von Infrastructure Deployment und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins 280
Upgrade von Windows-Agenten mit Hilfe von Infrastructure Deployment und des individuellen Agenten-Plug-ins 281
Upgrade von Linux- oder MacIntel-Agenten mithilfe von Infrastructure Deployment und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins 282
Upgrade von Linux- oder MacIntel-Agenten mithilfe von Infrastructure Deployment und des individuellen Agenten-Plug-in-Pakets 282
Upgrade von Linux- oder MacIntel-Agenten mithilfe von Software Delivery und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins 283
Upgrade von Linux- oder MacIntel-Agenten mithilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets 283
Upgrade von Unix-Agenten mit Hilfe von Infrastructure Deployment und des Pakets "AM, SD Plug-in(s)". 283
Upgrade von UNIX-Agenten mit Hilfe von Infrastructure Deployment und des individuellen Agenten-Plug-ins 284
Aktualisieren von Windows-Agenten mit Hilfe von Software Delivery und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins 284

Upgrade von Windows-Agenten mit Hilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets 285
Upgrade von UNIX-Agenten mit Hilfe von V und des Pakets "AM, SD Plug-in(s)". 285
Upgrade von UNIX-Agenten mit Hilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets 286

Kapitel 7: CA ITCM-Connector für CA Catalyst 287

Kapitel 8: Desktop-Virtualisierung 289

Vorbereiten von Golden Templates 290
Überprüfen der Voraussetzungen 291
Bereitstellen des DSM-Agenten im Golden Template 292
Installieren des CA DSM-Agent VDI-Support-Add-on-Pakets 293
Bereitstellen von Produktions-Softwarepaketen im Golden Template 294
Konfigurieren der Software-Neuinstallation 295
(Optional) Zuweisen von Scalability-Servern zu virtuellen Desktops 305
Konfigurieren der Inventarerfassung bei Software-Neuinstallation 306
Kennzeichnen der Vorlage und Erstellen eines Snapshots oder vDisks 307
Überprüfen der Golden Template-Zuweisung 308
Konfigurationsrichtlinien für die Unterstützung der Desktop-Virtualisierung 308
Aktualisieren von Golden Templates 317
Überprüfen der Voraussetzungen 318
Bereitstellen oder Entfernen von Software im Golden Template 318
(Für Xendesktop PVS) Konfigurieren der vDisk-Zielgerätepersönlichkeitsdaten 319
Anzeigen des vDisk-Inventars 321
Kennzeichnen der Vorlage nach der Aktualisierung 322
Aktualisieren der virtuellen Desktop-Gruppe oder des Pools 323
Überprüfen der Software-Aktualisierung des virtuellen Desktops 324
Verwalten von vDisks und vDisk-Klonen 324
Wie vDisk-Klone verarbeitet werden 324
Anzeigen der Beziehung zwischen Golden Template, Master-vDisk und Klonen 326
Verwalten von virtuellen Desktops von CA ITCM aus 328
Implementierungshandbücher für virtuelle Desktops 328
Anwenden von Sicherheits-Patches auf virtuellen Desktops 333
Anzeige des VDI-Inventars 337
Abfragen und Berichterstellung 338
Änderungen am Abfrage-Designer 338
Änderungen am DSM-Reporter 339
Ausschließen von Golden Images durch den Assistenten für veraltete Assets 339

Kapitel 9: Konfigurieren und Überwachen des CA ITCM-Infrastrukturzustands 341

Überprüfen der Voraussetzungen 342
Verstehen der HM-Architektur und -Grundlagen 343
Alarme und Alarmvorlagen 344
Systemüberwachungskomponenten 345
Externer Prozess-Manager (CAF-Plug-in) 347
Konfigurieren von Alarmen und Alarmvorlagen 348
Konfigurieren von Alarmen 349
Konfigurieren von Alarmvorlagen 352
Alarm-Collector konfigurieren 356
Festlegen von Alarm-Collector-Eigenschaften 357
Konfigurieren von Alarm-Aktionen 359
Festlegen der Alarmweiterleitungsdetails 362
Konfigurieren des Systemüberwachungs-Agenten 364
Konfigurieren der Einstellungen für das Hochladen von Alarmen 366
Konfigurieren der Servereinstellungen des Alarm-Collector 367
Konfigurieren von Proxyeinstellungen 368
Verwalten und Verfolgen des Status von Alarmen von WAC 369
Alarmreplikation 371

Kapitel 10: Konfigurieren und Authentifizieren von externen Verzeichnissen 373

Unterstützte externe Verzeichnisse 374
Überprüfen der Voraussetzungen 374
Hinzufügen eines Verzeichnisses zum Repository 375
Angeben der Verzeichnisserverdetails 376
Angeben von Informationen zur Verzeichnisbindung 377
Angeben von Details zum Basisverzeichnisknoten 377
Auswählen der Schemazuordnungsattribute 378
Verfeinern/Festlegen von Schemazuordnungsdetails 378
Überprüfen der Konfigurationsoptionen und Hinzufügen des Verzeichnisses 379
(Optional) Importieren eines Zertifikats (nur LDAPS) 380
Überprüfen des konfigurierten Verzeichnisses 381
(Optional) Aktualisieren des Verzeichnisses 381
Verzeichnis aktualisieren: Registerkarte "Einstellungen" 382
Verzeichnis aktualisieren: Registerkarte "Sicherheit" 384
Verzeichnis aktualisieren: Registerkarte "Schema" 384
Authentifizieren mithilfe des konfigurierten Verzeichnisses 385
Hinzufügen von Sicherheitsprofilen 385
Überprüfen der Verzeichnisauthentifizierung 388

Ändern der Richtlinie zur Verwendung eines anderen Formats für den Benutzernamen 390
Schemazuordnungsattribute 391
Verzeichnisintegration in CA IT Client Manager 400

Kapitel 11: CA ITCM-Sicherheitsfunktionen 403

Authentifizierung 403
Unterstützte Formate für Benutzernamen 405
X.509-zertifikatbasierte Authentifizierung 406
Sicherheit auf Objektebene und Zertifikate 406
Root-Zertifikate 407
Zertifikatspeicher 407
Basis-Hostidentitätszertifikate 407
Zertifikatverteilung 408
Erstellen neuer Zertifikate 409
Erstellen eines neuen Root-Zertifikats 409
Erstellen anwendungsspezifischer Zertifikate 410
Erstellen des Basis-Hostidentitätszertifikats 411
Installieren neuer Zertifikate 412
Installieren eines neuen Root-Zertifikats 412
Installieren anwendungsspezifischer Zertifikate 412
Installieren des Basis-Hostidentitätszertifikats. 413
Ersetzen von Zertifikaten 414
Entfernen eines Zertifikats 414
VMware-ESX-Sicherheit und Authentifizierung 415
Autorisierung 415
Sicherheitsprofile 417
Übersicht über Berechtigungen 418
Replikation 432
Einschränkungen 433
Sicherheitsszenario – Software Delivery 434
Konfigurieren von Common Security 436
So richten Sie die Sicherheitsfunktionen ein: 436
Sicherheitsprofile hinzufügen 437
Vordefinierte Zugriffstypen 439
Klassenberechtigungen angeben 441
Objektberechtigungen angeben 442
Gruppenberechtigungen angeben 443
Alle Berechtigungen 443
Unterstützung der Sicherheitsbereiche 444
Globale Einstellungen für Sicherheitsbereiche 445
Aktivieren der Sicherheitsbereicheinstellung für ein Sicherheitsprofil 445

Erstellen von Sicherheitsbereichen 446
Löschen von Sicherheitsbereichen 446
Verknüpfen von Sicherheitsbereichen mit Sicherheitsprofilen und Aufheben von Verknüpfungen 447
Verknüpfen von Sicherheitsbereichen mit gesicherten Objekten und Aufheben von Verknüpfungen 448
Konfigurieren der Verschlüsselung 448
Verschlüsselungsalgorithmen für die Kommunikation 449
Auswahl des entsprechenden Verschlüsselungsalgorithmus 450
Verschlüsselung in Umgebungen mit höchster Geheimhaltungsstufe 451
Kommunikation mit älteren Versionen (Kompatibilitätsrichtlinie) 451
FIPS-konforme Kryptographie 452
Bevor Sie den FIPS-Modus ändern 452
So wechseln Sie in "nur-FIPS" 454
So wechseln Sie in "FIPS-bevorzugt" 455
Ausführen des Konvertierungshilfsprogramms 456
Ändern Sie die Konfigurationsrichtlinie, um den FIPS-Modus zu ändern 458
Prüfen Sie den FIPS-Modus von DSM-Komponenten 460
Vordefinierte Abfragen und Berichte zum FIPS-Modus 461
Konfigurieren Sie FIPS-Compliance für DSM-Webkomponenten 461
Reparieren eines mit einer r12-Komponente verbundenen Agenten vom Typ "Nur-FIPS" 462
Szenarien Wenn Änderungen der FIPS-Richtlinie nicht in Kraft treten 463

Kapitel 12: ENC (Extended Network Connectivity) 465

Einführung in Extended Network Connectivity 465
ENC-Komponenten 467
Unterstützte Plattformen 467
ENC-Gateway-Verbindungsprozess 468
ENC-Gateway-Sicherheit 469
Authentifizierung 469
ENC-Gateway-Autorisierungsregeln 470
Allgemeine Begriffe 470
ENC und Uniform Resource Identifiers 472
Konfiguration von Autorisierungsregeln 473
Ereignisse 475
Verbindungssequenz 479
Virtuelle ENC-Verbindungen 480
Beispiel für das Festlegen von Regeln 481
Fragen zur Vorgehensweise 487
Auditing von Ereignissen 488
Installation und Konfiguration von ENC-Gateway-Komponenten 489
ENC- und SSA-Konfiguration 489
Aktivieren des ENC-Clients 490

Bereitstellung in einer ENC-Umgebung 490
ENC-Bereitstellungsszenarios 491
ENC-Bereitstellungsszenario – Das Pilotschema 491
ENC-Bereitstellungsszenario – Die Niederlassung 496
ENC-Bereitstellungsszenario – Kleines Outsourcing-Client-Unternehmen 500
ENC-Bereitstellungsszenario – Mittleres Outsourcing-Client-Unternehmen 501
ENC-Bereitstellungsszenario – Großes Outsourcing-Client-Unternehmen 502
Eigenständige ENC-Gateway-Router 503
Eigenständige ENC-Gateway-Server 504
Internet-Proxy-Unterstützung 504
Einschränkungen für die Verwendung von CA ITCM über ein ENC-Gateway 505
Verwenden des Hilfsprogramms "encUtilCmd" 507
Verwaltung von Zertifikaten 508
X.509-Zertifikate 509
Zertifikatsverwaltung mit einer PKI-Infrastruktur 509
Zertifikatsanforderungen 510
Die CA Technologies-Objekt-ID für die private Authentifizierung 511

Kapitel 13: Integration in CA Service Desk Manager 513

Service-Aware-Richtlinie 514
Ticket-Behandlung 515
Erkannte Assets mit eigenen Assets verknüpfen 515
Kontextabhängiger Start zwischen CA ITCM und CA Service Desk Manager 516
Kontextabhängiger Start von CA ITCM zu CA Service Desk Manager 516
Erstellen eines Tickets im Kontext eines verwalteten Assets (Ad-hoc) 518
Kontextabhängiger Start von CA Service Desk Manager zu CA ITCM 519
Einrichten von CA Service Desk Manager und CA ITCM 520
Voraussetzung für einen Start von CA Service Desk Manager innerhalb des Kontextes 520
Voraussetzungen für die CA Service Desk Manager-Integration in mehreren Engines 521
Voraussetzungen für die CA Service Desk Manager-Integration im Enterprise-Manager 521
Informationen zur CA ITCM- und CA Service Desk Manager-Integration 521
Software Delivery-Job von einem Enterprise-Manager, der für Service Desk aktiviert ist 522
Sichere Anmeldung beim CA Service Desk Manager-Webdienst 522
So konfigurieren Sie die sichere Anmeldung: 523
Benutzername- und Kennwortmethode (nicht verwaltet) 524
Zertifikat- oder eTrust PKI-Methode (verwaltet) 524
Einstellungen in der Konfigurationsrichtlinie 526

Kapitel 14: Fehlerbehebung 529

Freigabefehler der CIC-Verbindung 529
DSM-Engine stürzt bei angehaltener Datenbank ab 529

Voraussetzungen für SXP Packager unter Windows 8 530
Öffnen der exportierten Berichte 530
Fehler bei der Verbindung des Alarm-Collectors zum angegebenen Manager 531
Fehler bei der Verbindung des Alarm-Collectors mit der Datenbank 531
DSM-Explorer zeigt kein Aufforderungsfenster bei der Verbindung im Besprechungsmodus an 532
Probleme mit dem Ändern der Boot-Server-Konfiguration von "tftp" in den Zugriffsmodus "Freigabe" in Cluster-Setup 532
Problem mit Größendetails der ITCM- und CIC-Komponenten auf "Programme hinzufügen/entfernen" 533
Fehler und Verzögerungen beim Zugriff auf den technischem Support 533
SE-Linux-Support für CA ITCM-Komponenten 534
Unverständlicher Text auf der Benutzeroberfläche des japanischen Installationsprogramms 534
Problem mit Zeichenfolgen an der Eingabeaufforderung 535
Fehler beim Laden von gemeinsam genutzten Bibliotheken auf einem neueren 64-Bit-Linux-Betriebssystem 536
Agenteninstallation schlägt unter Solaris mit einem Fehler fehl 537
Remote Control unter Windows 8 Sicherer Modus 537
Verbindung mit MDB kann nicht hergestellt werden 538
Der DSM-Manager kann nach dem CAM-Upgrade nicht gestartet werden 538
Protokolle im temporären Ordner werden gelöscht 539
Stabilitätsprobleme des MDB-Installationsprogramms bei falscher Angabe der Variable "ORACLE_HOME" oder "ca_itrm Password" 539
Installationsfehler bei der benannte Instanz und der Port-ID 540
Antwortdatei enthält ungenutzte Einträge 540
Fehler bei der Synchronisierung von der SQL-MDB zur Oracle-Ziel-MDB 540
Fehler bei der Synchronisierung auf eine Ziel-MDB auf Oracle 541
Fehler bei der vereinheitlichten Anmeldung in der Webkonsole auf einem eigenständigen WAC 542
Hohe CPU-Auslastung nach DSM-Manager-Upgrade 543
Fehler bei der Infrastrukturbereitstellung bei vorhandenem virtuellen Computer unter Windows 2012 543

Anhang A: Automatisierungsdienst-Konfigurationsdatei 545

Anhang B: Von CA IT Client Manager verwendete Ports 551

Allgemeine Hinweise zur Port-Verwendung 552
Vom Enterprise-Manager verwendete Ports 552
Vom Domänen-Manager verwendete Ports 554
Von Infrastructure Deployment verwendete Ports 556
Vom Scalability-Server verwendete Ports 557
Vom Boot-Server verwendete Ports 559
Von der Engine verwendete Ports 559
Vom Agenten verwendete Ports 561
Vom Packager verwendete Ports 562

Von DSM-Explorer und -Reporter verwendete Ports 563
Vom ENC-Gateway verwendete Ports 564
Von der Quarantäne des AMT-Assets verwendete Ports 565
Verwendung von MDB-Ports 565

Anhang C: Software Delivery-Prozeduren zur Installation 567

Wichtige Hinweise zur Deinstallationsprozedur 568
CA DSM Agent + AM, RC, SD Plug-in(s) Linux (Intel) DEU 568
CA DSM Agent + Asset Management Plug-In Linux (Intel) DEU 568
CA DSM Agent + Basic Inventory Plug-In Linux (Intel) DEU 569
CA DMPrimer Linux (Intel) DEU 569
SMPackager (Linux) 569
CA DSM Remove Legacy Agent Linux (Intel) DEU 569
CA DSM Agent + Remote Control Plug-In Linux (Intel) DEU 569
CA DSM Agent + Software Delivery Plug-In Linux (Intel) DEU 570
CA DSM Scalability-Server Linux (Intel) DEU 571
CA DSM Agent + AM, RC, SD Plug-in(s) Win32 571
CA DSM Agent + Asset Management Plug-in 572
CA DSM Agent + Basic Inventory Plug-in 572
CA DSM Agent + Data Transport Plug-in 572
CA DSM Agent + Remote Control Plug-in 573
CA DSM Agent + Software Delivery Plug-in 574
CA DSM Constant Access (Intel AMT) 574
CA DSM eTrust PKI 575
CA DSM-Explorer 575
CA DSM Manager 575
CA DSM-Scalability-Server 576
CA DSM Secure Socket Adapter 576
CA DSM Remove Legacy Agent Win32 577

Anhang D: Aktuelle Zertifikate von CA IT Client Manager 579

Allgemeine Zertifikate 579
    Standard-DSM-Root-Zertfikat 579
    Standard-Basis-Hostidentitätszertifikat 580
Anwendungsspezifische Zertifikate 580
    Verzeichnissynchronisierungszertifikat 580
    Zertifikat für allgemeine Server-Registrierung 581
    CSM-Zertifikat 581
    Zertifikat für Mover des Software Delivery-Agenten 582
    Zertifikat für Software Delivery-Katalog 582
    Zertifikat für Enterprise-Zugriff 583

Zertifikat für Domänenzugriff 583
Zertifikat für Reporter-Zugriff 583

Anhang E: Verwendungsbeispiele für die Unterstützung von Sicherheitsbereichen 585

Unterstützung von Sicherheitsbereichen für Sicherheitsprofile 586
Anwendungsfall: Installieren von CA ITCM 586
Anwendungsfall: Aktualisierung einer vorhandenen Installation 587
Verwendungsbeispiele: Sicherheitsprofile 587
Anwendungsfall: Erstellen eines Sicherheitsprofils 588
Anwendungsfall: Ändern von Bereichseinstellungen für ein Sicherheitsprofil 588
Anwendungsfall: Löschen eines Sicherheitsprofils 589
Verwendungsbeispiele: Computer 589
Anwendungsfall: Manuelles Erstellen eines Computerobjekts 589
Anwendungsfall: Ein neuer DSM-Agent wurde gefunden 590
Verwendungsbeispiele: Asset-Gruppen 590
Anwendungsfall: Erstellen einer Asset-Gruppe 591
Anwendungsfall: Hinzufügen eines Computers zu einer Asset-Gruppe 592
Anwendungsfall: Entfernen eines Computers aus einer Asset-Gruppe 593
Anwendungsfall: Ändern der Bereichsberechtigung einer Asset-Gruppe 594
Anwendungsfall: Deaktivieren der Übernahme und Zurücksetzung 594
Verwendungsbeispiele: Abfragen 595
Anwendungsfall: Erstellen einer Abfrage 595
Anwendungsfall: Ausführen einer Abfrage 596
Anwendungsfall: Ausführen einer Abfrage im Kontext von Software Delivery 596
Verwendungsbeispiele: Softwarepakete 597
Anwendungsfall: Erstellen von Softwarepaketen 597
Verwendungsbeispiele: Softwareprozeduren 597
Anwendungsfall: Erstellen einer Softwareprozedur 598
Verwendungsbeispiele: Softwaregruppen 598
Anwendungsfall: Erstellen einer Softwaregruppe 598
Verwendungsbeispiele: Softwarerichtlinien 599
Anwendungsfall: Erstellen einer Softwarerichtlinie 599
Verwendungsbeispiele: Softwarejobs 599
Anwendungsfall: Erstellen von Softwarejobs 600
Verwendungsbeispiele: Asset-Jobs 600
Anwendungsfall: Erstellen eines Asset-Jobs 600
Verwendungsbeispiele: Engine-Tasks 601
Anwendungsfall: Erstellen eines Engine-Tasks 601
Verwendungsbeispiele: Verwalten von Bereichen 601
Anwendungsfall: Erstmaliges Aktivieren der Bereichscodeunterstützung 602

Anwendungsfall: Deaktivieren der Bereichscodeunterstützung 602
Anwendungsfall: Erneutes Aktivieren der Bereichscodeunterstützung 603
Anwendungsfall: Ändern der Standardbereichsberechtigungen 603
Anwendungsfall: Hinzufügen eines neuen Bereichs 604
Anwendungsfall: Löschen eines Bereichs 604
Anwendungsfall: Als Eigentum übernehmen 604

Anhang F: CAF Geplante Jobs 605

CAF-Standardjobs und -parameter 605
Beispiele für geplante CAF-Jobs 608

Anhang G: FIPS 140-2-Konformität 609

FIPS PUB 140-2 609
Referenzen 610
Unterstützte FIPS-Modi 610
Kryptographisches Modul – RSA Crypto 611
Kryptographische Sicherheitsfunktionen 611
Komponentenspezifische Verwendung von Kryptographie 613
FIPS-Konformität von CA ITCM-externen Komponenten 614
Microsoft Windows-Betriebsumgebungen 615
SQL Server 615
Andere Komponenten 615
Nicht genehmigte Verwendung von Sicherheitsfunktionen 616

Terminologieglossar 617

Kapitel 1: Funktionsweise von CA ITCM

CA IT Client Manager ist eine plattformübergreifende IT-Ressourcenmanagement-Lösung, die hochmoderne, nahtlos integrierte Asset Management-, Software Delivery- und Remote Control-Funktionalität für jedes Unternehmen bietet.

Dieses Kapitel enthält folgende Themen:

DSM-Architektur (siehe Seite 21)
DSM-Explorer (siehe Seite 24)
Webkonsole (siehe Seite 25)
Manager (siehe Seite 26)
Scalability-Server (siehe Seite 38)
Agent (siehe Seite 42)
DSM Reporter (siehe Seite 47)
Unterstützte Betriebsumgebungen (siehe Seite 47)
Common Application Framework (siehe Seite 48)
Allgemeine Konfiguration (siehe Seite 52)
Inventarisierung und Verwaltung von Geräten (siehe Seite 71)

DSM-Architektur

CA IT Client Manager bietet eine gemeinsame Oberfläche und Architektur für Asset Management-, Software Delivery- und Remote Control-Funktionen (DSM-Architektur), wobei die Integration jedoch über die Verwaltungs-Benutzeroberfläche hinausreicht.

Kernelemente der Infrastruktur werden von allen Asset Management-, Software Delivery- und Remote Control-Funktionen und -Komponenten gemeinsam genutzt. Wenn Sie z. B. zwei oder alle Funktionalitäten installieren, sind Datenbank, Kommunikation, Prozesssteuerung, Protokollierung, Event Management und andere Aspekte gleichmäßig strukturiert. Dadurch stehen Ihnen bei allen installierten Funktionalitäten nützliche Funktionen und eine konsistente Terminologie, Architektur, Oberfläche sowie Daten zur Verfügung.

Zusätzlich weist die DSM-Architektur mehrere konsistente und allgemeine Konzepte auf, die ebenfalls von allen Asset Management-, Software Delivery- und Remote Control-Funktionalitäten verwendet werden. Dazu gehören folgende gemeinsam verwendete Elemente:

- Grafische Benutzeroberfläche (GUI)
- Manager
- Scalability-Server
- Agent

Die DSM-Architektur besteht aus den folgenden Ebenen:

DSM-Explorer/Webkonsole

Ermöglichen die administrative Steuerung von CA ITCM und den dazugehörigen Komponenten-Plug-ins. Der DSM-Explorer ist die grafische Benutzeroberfläche für Windows, und die Webkonsole ist eine browserbasierte GUI für Windows und Linux.

Enterprise-Manager

Bietet eine zentrale Verwaltungsstelle für mehrere Domänen.

Domänen-Manager

Stellt alle Managementdienste für die niedrigeren Ebenen und Agenten bereit.

Scalability-Server

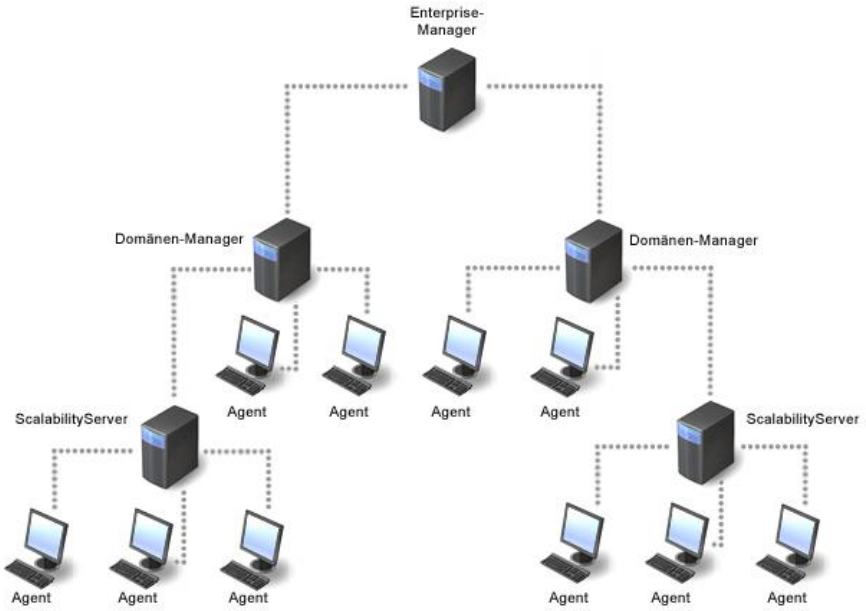
Agiert als Verteilungsstelle für die Software Delivery- und Softwareverteilungs-Aktionen und als Erfassungsstelle für das Asset-Inventar.

Agent

Bietet auf unterstützten Hosts Remote Control-, Software Delivery- und Asset-Inventardienste.

Jede Managerebene ist ein Host für eine Instanz der Management-Datenbank (MDB).

Die folgende Beispielabbildung stellt die mehrschichtige Architektur dar. In diesem Beispiel dient ein Enterprise-Manager als Verwaltungspunkt für zwei Domänen-Manager, die jeweils direkt verbundene Agenten und einen untergeordneten Scalability-Server verwalten. Die Scalability-Server verwalten die Tasks zwischen den Agenten- und Domänen-Manager-Ebenen.



DSM-Explorer

Der DSM-Explorer ist die zentrale Verwaltungsoberfläche für CA ITCM in Windows-Betriebsumgebungen.

Die DSM-Explorer-Leiste auf der linken Seite bietet vier Ansichten: Baumansicht, Verlauf, Lesezeichen und Suche. Die Baumansicht ist die Standardansicht und enthält die Hauptnavigation zu den verschiedenen Funktionen des DSM-Explorers.

Bei Auswahl in der Baumansicht bieten zahlreiche Baumknoten Listen in der Ansicht auf der rechten Seite.

Viele Knoten bieten außerdem eine grafische, webbasierte Darstellung. Das Hauptportal ist ein Beispiel hierfür. Es bietet eine systemweite Übersicht von CA ITCM über vier Portlets:

Hauptfunktionen

Bietet Zugriff auf die Hauptbereiche von DSM-Explorer, z. B. auf "Computer und Benutzer", "Software", "Jobs" usw.

Häufig verwendet

Zugriff auf die am häufigsten navigierten Baumknoten.

Systemstatus

Zeigt Informationen zur Domäne an, mit denen eine Verbindung besteht, beispielsweise Statistik, Fehlschläge und aktive Tasks.

Schnellstart

Bietet schnellen Zugriff auf die meist verwendeten Funktionen.

Sie können die Portlets "Systemstatus" und "Schnellstart" Ihren Anforderungen anpassen.

Im rechten Fensterbereich des DSM-Explorers steht ein Tutorial zur Verfügung. Im Tutorial werden Informationen zum Navigieren des DSM-Explorers und die ersten Schritte mit den am häufigsten ausgeführten Tasks dargestellt. Das Tutorial kann mit der DSM-Explorer-Funktion "Ansicht", "Tutorial-Leiste" aktiviert und deaktiviert werden.

Weitere Informationen und kontextabhängige Hilfe finden Sie in der *Online-Hilfe zu DSM-Explorer*.

Webkonsole

Die Webkonsole ist eine browserbasierte Benutzeroberfläche für CA IT Client Manager, die unter Windows und Linux/UNIX installiert werden kann.

Die Webkonsole kann auf demselben Computer wie der Manager oder auf einem anderen Computer installiert werden (Remote-Webkonsole).

Webkonsolen-Zugriff

Zum Zugreifen auf die Webkonsole öffnen Sie einfach einen Browser und geben in der Adressleiste folgende URL ein:

`http://MyManager/wac`

MyManager steht für den DNS-Namen, den Hostnamen oder die IP-Adresse des Computers, auf dem die Webkonsole installiert ist. Webkonsole meldet Sie automatisch mit den Anmeldeinformationen an, die Sie bei der Anmeldung bei diesem Computer angegeben haben. Auf der Anmeldeseite der Webkonsole befindet sich ein Dropdown-Feld, mit dem Sie einen anderen Manager angeben können.

Funktionen der Webkonsole

In der Webkonsole können Sie über ein leistungsfähiges, aber einfaches Suchfenster auf DSM-Objekte zugreifen. Wenn Sie ein Objekt gefunden haben, bietet die browserbasierte Oberfläche zahlreiche Funktionen über Registerkarten, Portlets, Seitenabschnitte und Navigationslinks.

Die Webkonsole bietet dem Benutzer eine umfassende Ansicht der DSM-Informationen. Abhängig von den installierten Produkten und Komponenten kann es sich um folgende Informationen handeln:

- Computer
- Gruppen
- Anwender
- Softwarepakete
- Softwaredefinitionen
- Jobs
- Richtlinien
- Abfragen
- Alarme

Über die Webkonsole können Benutzer auch folgende Aktivitäten durchführen (wenn die entsprechenden Produkte und Komponenten installiert wurden):

- Computer erstellen und löschen
- Gruppen erstellen, ändern und entfernen
- BS-Installationsjobs
- Software installieren
- Software deinstallieren
- Softwareinstallationsjobs konfigurieren
- Überwachen Sie und verfolgen Sie Systemüberwachungsalarme.

Die Webkonsole kann im Kontext eines Jobs oder einer Richtlinie über einen URL von einer anderen Anwendung aus gestartet werden, die Zugriff auf die UUID eines entsprechenden Objekts hat.

Die Webkonsole kann auch die Anwendung CA Service Desk Manager starten, wenn ein Ticket (Problem) vorliegt, das sich auf einen Richtlinienverstoß oder einen fehlgeschlagenen Software-Job bezieht.

Unterstützte Web-Browser und Webserver

Informationen zur Unterstützung von Webservern und Browsern finden Sie in der Kompatibilitätsmatrix.

Manager

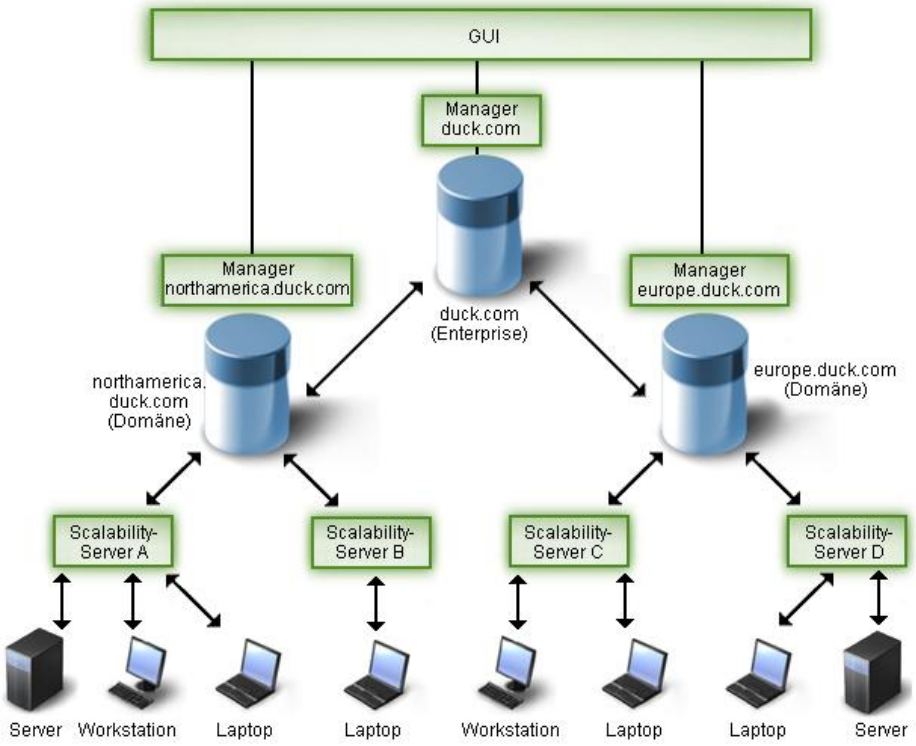
Folgende Aspekte der Manager-Rolle in CA ITCM werden behandelt:

- Enterprise- und Domänenkonzept (siehe Seite 27)
- Enterprise- und Domänenkomponenten (siehe Seite 28)
- Engine-Konzept (siehe Seite 31)

Enterprise- und Domänenkonzept

CA ITCM verfügt über zwei Managementebenen: die Domänen- und die Enterprise-Ebene. Auf beiden Ebenen sind Management-Datenbanken vorhanden. Wenn in einer Organisation mehrere Domänen bereitgestellt werden, kann ein Enterprise als alleinige Managementstelle bereitgestellt werden.

Die folgende Abbildung zeigt ein Beispiel für eine Architektur mit zwei Ebenen, die aus dem Enterprise-Manager des Unternehmens und zwei Domänen-Managern besteht, mit denen jeweils zwei Scalability-Server verbunden sind:



Der Enterprise-Manager mit dem Namen "duck.com" und zwei Domänen-Manager, einer für die Verwaltung von Aufgaben und Geräten in der Region Nordamerika (northamerica.duck.com) und der andere für die Verwaltung von Aufgaben und Geräten in der Region Europa (europe.duck.com). Mit den Domänen-Managern sind jeweils zwei Scalability-Server verbunden, die die Auslastung der Domänen-Manager verringern, indem sie Endbenutzergeräte, wie z. B. Laptops und Workstations, sowie weitere Server verwalten.

Enterprise- und Domänenkomponenten

Die folgende Liste enthält Begriffe und Definitionen, die für das Verständnis des Enterprise- und Domänenkonzepts von CA IT Client Manager bedeutsam sind.

Enterprise-Manager

Ein *DSM-Enterprise-Manager* ist eine optionale oberste Managementebene für CA IT Client Manager. Er bietet zentrale Managementfunktionen für eine Gruppe von DSM-Domänen und ermöglicht darüber hinaus das Festlegen von Konfigurationen und Richtlinien für Objektgruppen in einer oder mehreren Domänen. In einer DSM-Umgebung kann nur ein Enterprise-Manager vorhanden sein.

Domänen-Manager

Ein *DSM-Domänen-Manager* bietet zentrale Funktionen für das Management der anderen DSM-Komponenten, einschließlich der Scalability-Server und Agenten.

Scalability-Server

Ein *DSM-Scalability-Server* ist ein verteilter Prozess, der als primäre Schnittstelle für den Agenten agiert. Mit Scalability-Servern wird die DSM-Auslastung auf zahlreiche Hosts verteilt.

Engine

Eine *DSM-Engine* ist ein Prozess, der Kommunikationsdienste zwischen Scalability-Servern und ihren übergeordneten DSM-Domänen- und Enterprise-Managern ermöglicht.

Die Management-Datenbank im Enterprise- und Domänen-Konzept

Die Produktsuites von CA Technologies werden über ein gemeinsames Repository für Enterprise-Daten integriert, die so genannte Management-Datenbank (MDB). Die MDB bietet eine einheitliche Struktur für die Speicherung der Managementdaten aller CA Technologies-Produkte. Die MDB integriert Managementdaten aus allen IT-Bereichen und CA Technologies-Produkten. Kunden und Partner können die MDB erweitern, um zusätzliche IT-Managementdaten aus Softwareprodukten und Tools zu berücksichtigen, die nicht von CA sind.

CA IT Client Manager basiert auf MDB r1.5 SP1, bei dem standardmäßig nur die allgemeinen Asset- und DSM-Schemata installiert werden. Wenn ein weiteres CA-Produkt die von CA ITCM erstellte MDB verwenden soll und MDB r1.5 von diesem Produkt unterstützt wird, wird dessen Schema über die vorhandene MDB installiert.

Wenn das Folgeprodukt jedoch nur MDB r1.0.4 unterstützt, schlägt die Installation fehl. Ist dies der Fall, aktivieren Sie die Option “Kompatibilitätsmodus”, bevor Sie die MDB installieren. CA ITCM installiert zunächst die aktuellen MDB r1.0.4 Patches und aktualisiert anschließend die MDB auf MDB r1.5. Dadurch sind alle Schemadefinitionen vorhanden, und nur die Schemadefinitionen für allgemeine Assets und DSM befinden sich auf derselben Ebene wie die für MDB r1.5. Weitere Informationen hierzu finden Sie unter Vorbereitung für das Arbeiten mit einer Microsoft SQL Server-MDB (siehe Seite 126) oder unter Vorbereitung für das Arbeiten mit einer Oracle-MDB (siehe Seite 129).

Allgemeine Informationen zur MDB, einschließlich der Bereitstellung und Verwaltung, finden Sie in der *MDB-Übersicht*, die in der CA IT Client Manager-Dokumentation (Bookshelf) enthalten ist.

In der Multi-Tier-Architektur können Instanzen der Management-Datenbank (MDB) auf der Enterprise- und der Domänen-Manager-Ebene implementiert werden. Auf beiden Ebenen werden Microsoft SQL Server- und Oracle-MDBs unterstützt. Sie können zudem MDBs unterschiedlicher Datenbank-Provider auf den verschiedenen Ebenen implementieren, z. B. können Sie SQL Server als Domänen-Manager und Oracle als Enterprise-Manager auswählen..

In gemischten Konfigurationen, z. B. bei einem Domänen-Manager mit SQL Server-basierter MDB und einem Enterprise-Manager mit Oracle-basierter MDB, benötigen Sie die entsprechenden Datenbank-Clients auf den Managern. In diesem Beispiel wären dies der Oracle-Client auf dem Domänen-Manager und der SQL-Client auf dem Enterprise-Manager.

Derzeit wird eine Oracle-basierte MDB nur als Remote-Datenbank auf einem Computer mit einer Sun Solaris-Betriebsumgebung unterstützt. Weitere Informationen zu den derzeit unterstützten Datenbankversionen und Betriebsumgebungen finden Sie in den *Versionshinweisen zu CA IT Client Manager*, die in der CA IT Client Manager-Dokumentation (Bookshelf) enthalten sind.

Die folgenden Datenbankszenarios werden unterstützt:

Lokale SQL Server-MDB

DSM-Domänen- oder Enterprise-Manager unter Windows, wobei sich die MDB auf demselben Computer befindet und auf SQL Server basiert.

SQL Server-Remote-MDB

DSM-Domänen- oder Enterprise-Manager unter Windows, wobei sich die MDB auf einem Remote-Server-Computer mit dem Betriebssystem Windows befindet und auf SQL Server basiert.

Oracle-Remote-MDB

DSM-Domänen- oder Enterprise-Manager unter Windows, wobei sich die MDB auf einem Remote-Server-Computer mit dem Betriebssystem Solaris befindet und auf Oracle basiert.

Alle MDBs in der Enterprise- und Domänenstruktur sind nach dem gleichen Schema aufgebaut. Alle Domänendatenbanken enthalten Informationen zum Aufbau der Verbindung mit dem Enterprise-Manager. Die Enterprise-Datenbank enthält Informationen zum Herstellen der Verbindung zu allen Domänen, die mit ihr verknüpft sind, sowie zu den verfügbaren Managern und ihrem Speicherort.

CA ITCM enthält eine Funktion, mit der Sie die in einer Microsoft SQL Server-MDB auf einer Domäne oder in Enterprise-Manager gesammelten Daten mit den Daten einer Remote SQL Server- oder Oracle-MDB synchronisieren können. Diese Datenbanksynchronisierungsfunktion unterstützt beispielsweise vorhandene Installationen von CA Technologies Service Desk Manager- und Asset Portfolio Management-Produkten, die eine SQL Server- oder Oracle-MDB verwenden. Weitere Informationen zur Synchronisierungsfunktion finden Sie unter Datensynchronisierung zwischen einer MDB und einer separaten Ziel-MDB (siehe Seite 35).

Hinweis: Zur vollständigen Unterstützung der Unicenter Asset Portfolio Management-Produktintegration müssen Sie den Patch RO02252 installieren. Installationsanweisungen finden Sie in der Readme-Datei zu Unicenter Asset Portfolio Management, RO02252. Weitere Informationen zu Unicenter Asset Portfolio Management und CA Service Desk Manager finden Sie in der Dokumentation zum jeweiligen Produkt.

MDB-Installation

Die Management-Datenbank (MDB) kann lokal auf dem Manager oder als Remote-MDB auf einem gesonderten Computer installiert werden, abhängig von den Anforderungen an Skalierbarkeit und Leistung. Die Installation der MDB unter Windows und Solaris wird von den DSM-Installationskits unterstützt.

Ausführliche Informationen zur MDB-Installation finden Sie im Abschnitt Management-Datenbank (MDB) (siehe Seite 116) im Kapitel "Installation von CA ITCM".

MDB-Verwaltung

Zur Pflege des Zustands und der Leistung der Management-Datenbank (MDB) ist die Datenbankverwaltung unerlässlich. Um Sie bei dieser Aufgabe zu unterstützen, stellt CA Technologies auf dem CA IT Client Manager-Installationsmedium (DVD) MDB-Wartungsskripte zur Verfügung.

Weitere Informationen zu MDB-Wartungsskripten finden Sie im Abschnitt Management-Datenbank (MDB) (siehe Seite 116) im Kapitel "Installation von CA ITCM". Außerdem sind die spezifischen Anforderungen der MDB-Verwaltung hinsichtlich Konfiguration und Wartung in der *MDB-Übersicht* in der CA IT Client Manager-Dokumentation (Bookshelf) beschrieben.

Engine-Konzept

Eine Engine ist ein Prozess, der Kommunikationsdienste zwischen Scalability-Servern und dem Domänen-Manager und der Management-Datenbank bereitstellt.

Eine Engine verfügt über folgende Funktionen:

- Erfassen des Computerinventars von einem Scalability-Server.
- Schreiben von Konfigurationsdaten auf einen Scalability-Server.
- Kopieren von Daten zwischen Enterprise- und Domänendatenbanken (Replikation).
- Ausführen einer Evaluierung einer dynamischen Abfragegruppe.
- Ausführen von Aktionen, die sich auf die Evaluierung der Gruppenabfrage beziehen.
- Ausführen geplanter Berichte.
- Kommunizieren des Status des Inventarjobs.

Aspekte der Engine-Verwaltung

Der Status der Engine-Tasks kann über den DSM-Explorer angezeigt werden. Dort können Sie Engine-Tasks hinzufügen, ändern und löschen.

Jede Instanz eines Domänen- und Enterprise-Managers enthält eine Standard-Engine namens "System-Engine".

Sie können zusätzliche Engines installieren, um die Auslastung der Standard-Engine zu senken.

Wenn ein neuer Scalability-Server bereitgestellt wird, wird immer automatisch ein Engine-Erfassungstask erstellt und für die standardmäßige System-Engine geplant. Zur Behandlung dieses Tasks können Sie während der Installation des Scalability-Servers eine andere Engine zuweisen.

Wenn ein Domänen-Manager mit einem Enterprise-Manager verknüpft wird, wird immer automatisch ein Engine-Replikationstask erstellt und mit der standardmäßigen System-Engine verknüpft.

Informationserfassung

Der Haupt-Task einer Engine besteht im Erfassen von Asset-Informationen von Scalability-Servern.

Wenn ein DSM-Agent zum ersten Mal eine Verbindung zu einem Scalability-Server herstellt, übermittelt er eine Anforderung zum Erstellen eines ersten Inventars und von Systeminformationen. Anschließend speichert er beide.

Wenn eine Engine eine Verbindung zu einem Scalability-Server herstellt, führt sie folgende Tasks aus:

1. Prüft die Integrität des Scalability-Servers.
2. Legt fest, ob Agenten zum ersten Mal eine Verbindung zu diesem Server herstellen.
3. Wenn die Assetsn im gesamten System neu sind, werden sie in der Datenbank erstellt.
4. Verarbeitet alle Inventarinformationen, die von den vorhandenen Agenten bereitgestellt werden.

Die erfassten Informationen können folgende Formate haben:

- Inventar (Hardware- oder Vorlageninformationen)
- Softwareinventar (heuristisch oder auf Basis der Signaturdateien)
- Konfigurationsdateien ("autoexec.bat" oder andere INI-Dateien, die für die Sicherung konfiguriert sind.)
- Jobstatus
- Modulstatus
- Datum und Uhrzeit der letzten Ausführung des Agenten
- Überwachungsdaten zur Softwareverwendung
- Informationen zur Beziehung (zwischen Computern, Benutzern und Geräten)

Datenreplikation zwischen Enterprise und Domäne

Eine weitere Aufgabe der Engine ist die Behandlung der Replikation von Daten zwischen Domänen- und Enterprise-Datenbanken. Die Replikation von der Management-Datenbank auf dem Domänen-Manager mit der Management-Datenbank auf dem Enterprise-Manager wird von einem Replikationsjob ausgeführt, der über den Engine-Prozess des Domänen-Managers ausgeführt wird.

Wenn die Replikation startet, legt die Engine fest, welche Informationen vom Domänen- zum Enterprise-Manager gepusht werden müssen. Außerdem wird festgelegt, welche Informationen vom Enterprise-Manager zum Domänen-Manager abgerufen werden.

Normalerweise werden hostspezifische Informationen, z. B. Inventarattribute, aufwärts repliziert, während Konfigurationsinformationen, wie beispielsweise Asset-Gruppen, abwärts repliziert werden.

Mit jedem Domänen-Manager wird auch eine Standard-Engine installiert. Wenn der Domänen-Manager mit einem Enterprise-Manager verknüpft wird, wird diese Engine konfiguriert, Replikationstasks von Domäne zum Enterprise durchzuführen.

Replizierte Datenbankobjekte

Die folgende Tabelle enthält die Datenbankobjekte, die vom Enterprise-Manager zum Domänen-Manager (abwärts) und vom Domänen-Manager zum Enterprise-Manager (aufwärts) repliziert werden.

Objekt	Richtung der Replikation
Erkannte Computer	aufwärts
Erkannte Benutzer	aufwärts
Erkannte Computerbenutzer (Beziehungen zwischen Computer und Benutzern)	aufwärts

Objekt	Richtung der Replikation
Remote Control-Adressbuchcomputer	abwärts
Definitionen externer Assets	abwärts
Externe Assets	aufwärts
Allgemeines Computerinventar	aufwärts
Zusätzliche Inventarkomponenten **Hinweis:** Standardmäßig werden diese Objekte nicht repliziert. Sie können die Replizierung aktivieren bzw. deaktivieren, indem Sie mit der rechten Maustaste auf den Knoten "Inventar/Sonstiges/<*Modulname*> des Agenten klicken und die Option "Replikation von Heuristisch auf Enterprise" auswählen. Die geänderte Konfiguration gilt für alle Computer in dieser Gruppe.	aufwärts
Inventar externer Assets	aufwärts
Abfragedefinitionen	abwärts
Definitionen der Gruppen	abwärts
Gruppenzugehörigkeit	abwärts
Benutzerdefinierte Softwaredefinitionen	abwärts
Benutzerdefinierter Hersteller	abwärts
Enterprise-Manager-Eigenschaften	abwärts
Domänen-Manager-Eigenschaften	aufwärts
Softwareinventar für Computer (auf Grundlage des Signatur-Scans gefunden)	aufwärts
Beim heuristischen Scan erkanntes Softwareinventar **Hinweis:** Standardmäßig wird dieses Objekt nicht repliziert. Sie können die Replizierung aktivieren bzw. deaktivieren, indem Sie mit der rechten Maustaste auf den Knoten "Software/Erkannt" klicken und die Option "Replikation von Heuristisch auf Enterprise" auswählen. Die geänderte Konfiguration gilt für alle Computer in dieser Gruppe.	aufwärts
Asset Management-Jobs	abwärts
Status des Asset Management-Jobs	aufwärts
Asset Management-Module	abwärts
Status des Asset Management-Moduls	aufwärts
Konfigurationsdatei-Definitionen von Asset Management	abwärts
Konfigurationsdateien von Asset Management **Hinweis:** Diese Dateien werden nur auf dem Enterprise-Manager repliziert, wenn auf dem Enterprise-Manager die Anforderung zum Erfassen dieser Informationen definiert wurde. Wenn die Anforderung auf dem Domänen-Manager definiert wurde, werden die Dateien nicht aufwärts repliziert.	aufwärts

Objekt	Richtung der Replikation
Asset Management-Vorlagendefinitionen	abwärts
Asset Management-Richtliniendefinitionen	abwärts
Systemüberwachungsalarme	aufwärts

Datensynchronisierung zwischen einer MDB und einer separaten Ziel-MDB

Für manche Implementierungen wird von den Kunden gewünscht, dass CA Technologies-Produkte wie Service Desk und Asset Portfolio Management separate bzw. andere Management-Datenbanken (MDBs) verwenden als die Datenbank, die der DSM-Manager verwendet.

Diese CA Technologies-Produkte sind jedoch in vielerlei Hinsicht für ihre Asset Management-Aufgaben von CA ITCM-Daten abhängig.

Daher bietet CA ITCM Manager-Funktionen, die die von CA ITCM erkannten Daten unterstützen und mit einer separaten MDB synchronisieren, die auf Microsoft SQL Server (SQL Bridge) oder Oracle (Oracle Bridge) basieren kann. Die Synchronisierungsfunktionen synchronisieren CA ITCM-Assets und -Inventardaten, die in einer SQL Server-MDB auf dem DSM-Domänen- oder Enterprise-Manager unter Windows erfasst werden, mit den entsprechenden Daten in der Ziel-SQL Server- bzw. Oracle-MDB.

Die Synchronisierung wird von einem Engine-Task zu einer geplanten Zeit initialisiert. Sie erstellen diesen Engine-Task und definieren die Zeitplanung für den Task mit Hilfe des Assistenten zur Erstellung von Engine-Tasks in der GUI des DSM-Explorers. Eine separate Engine kann die Synchronisierung auf einem Remote-Computer durchführen.

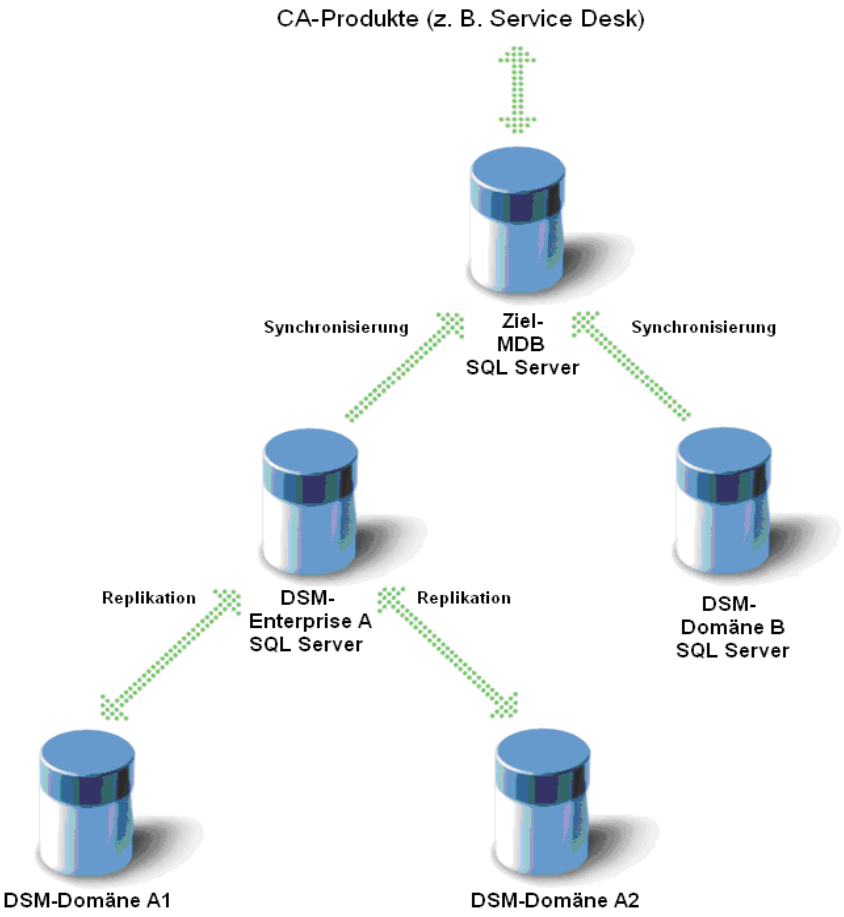
Ausführlichere Informationen finden Sie im Abschnitt Management-Datenbank (MDB) (siehe Seite 116) im Kapitel "Installation von CA ITCM".

Architektur des Synchronisierungsmechanismus

Der Synchronisierungsmechanismus ähnelt dem Replizierungsmechanismus, der zwischen dem DSM-Domänen-Manager und dem Enterprise-Manager verwendet wird.

Die Synchronisierung wird in eine Richtung ausgeführt, von den Managern zur Ziel-MDB. Dies bedeutet, wenn synchronisierte Daten auf der Ziel-MDB von einem anderen Prozess geändert werden, werden sie überschrieben, wenn der entsprechende Datensatz über die Synchronisierungsmethode von der MDB des Managers auf die Ziel-MDB verschoben wird.

Die folgende Abbildung zeigt ein spezielles Szenario, in dem die Synchronisierung von einem Enterprise-Manager und von einem Domänen-Manager, die beide ihre MDBs unter Microsoft SQL Server beherbergen, mit einer SQL Server-Ziel-MDB ausgeführt wird.



In einem anderen Szenario basiert die Ziel-MDB möglicherweise auf Oracle. Es ist auch möglich, eine SQL Server-MDB auf einem Enterprise- oder Domänen-Manager mit zwei verschiedenen Ziel-MDBs zu synchronisieren.

Unterstützte Datenbank-Szenarios

Unter Kompatibilitätsmatrix finden Sie Informationen in Bezug auf die SQL Bridge- und Oracle Bridge-Synchronisierungsfunktionsunterstützung.

Unterstützte Datenbankszenarien für SQL Bridge und Oracle Bridge

Wenn Sie CA Service Desk Manager oder CA IT Asset Manager auf einer MDB installiert haben, die auf SQL Bridge oder Oracle Bridge basiert, können Sie die von ihnen aufgefüllten Mandanteninformationen in die CA ITCM-Datenbank synchronisieren.

- Unter Kompatibilitätsmatrix finden Sie Informationen in Bezug auf für SQL Bridge- und Oracle Bridge-Synchronisierungsfunktionen unterstützte Datenbankszenarien.

Unterstützung für CA Technologies-Produkte

Unter Kompatibilitätsmatrix finden Sie Informationen in Bezug auf SQL Bridge- und Oracle Bridge-Synchronisierungsfunktionen für SQL Server- und durch Oracle-basierte MDBs unterstützte CA Technologies-Produkte, CA Service Desk Manager und Unicenter Asset Portfolio Management:

- **SQL Bridge:**

  Damit SQL Bridge vollständig genutzt werden kann, muss der Testfix T5D6008 für Windows auf die Computer angewendet werden, auf denen CA Service Desk Manager r11.2 und Unicenter Asset Portfolio Management r11.3 installiert ist. Der Testfix ist auf der CA Support Online-Website verfügbar. Laden Sie den Testfix herunter und befolgen Sie die ausführlichen Installationsanweisungen in der Readme-Datei, die mit dem Testfix zur Verfügung gestellt wird.

- **Oracle Bridge:**

  Damit Oracle Bridge vollständig genutzt werden kann, muss ein neuer Parameter, "dsm_oracle_ddl", zur AMS.Properties-Datei für CA Service Desk Manager hinzugefügt werden, um Oracle Bridge zu aktivieren:

  ```
  dsm_oracle_ddl=1
  ```

Weitere Informationen zur Installation von SQL Bridge und Oracle Bridge in Ihrer Anwendungsumgebung finden Sie in den Abschnitten Installation von SQL Bridge (siehe Seite 223) und Installation von Oracle Bridge (siehe Seite 224).

Scalability-Server

In CA ITCM bietet ein Scalability-Server die Schnittstelle zwischen den Agenten und ihrem Domänen-Manager.

Auf der untersten Ebene ermöglicht ein Scalability-Server die Verteilung der Auslastung der zu verwaltenden einzelnen Agenten auf mehrere Hosts. Die Last kann über mehrere Scalability-Server verteilt werden, statt alle Agenten direkt mit einem einzelnen Manager kommunizieren zu lassen. Softwarepakete werden beispielsweise auf einem Scalability-Server durch Staging bereitgestellt, bevor sie auf Endsysteme heruntergeladen werden. Inventar kann auf dem Scalability-Server gespeichert werden, bevor es auf den Manager hochgeladen wird.

Mit virtuellen Anwendungen funktioniert der Scalability-Server auch als Streaming-Server für Pakete mit virtuellen Anwendungen, die per Datenstrom an Computer mit Windows-Betriebssystem übertragen werden.

Ein Scalability-Server besteht aus einer Reihe von Systemprozessen, die ohne sichtbare Benutzeroberfläche im Hintergrund ausgeführt werden.

Unterkomponenten einer Scalability-Server-Basisinstallation

Die Basisinstallation eines Scalability-Servers besteht aus den folgenden Unterkomponenten:

- Application Framework (mit Registrierungsfunktion)
- Allgemeine Serverfunktionalität

  Der Scalability-Server kann Registrierungsanforderungen und einfache Inventarinformationen von Agenten empfangen, sich bei Managern registrieren sowie verschiedene Managementinformationen und Benachrichtigungen vom Manager empfangen und an ihn übermitteln.
- Dateispeicherdatenbank

  Die Dateispeicherdatenbank ist ein lokales Repository, mit dem der Scalability-Server die Informationen speichert, die zum Bedienen der Agenten benötigt werden. In einer Scalability-Server-Minimalinstallation besteht die Dateidatenbank aus einem Wörterbuch registrierter Agenten und dem Basisinventar, zu denen diese Agenten Berichte erstellen.

Tasks des Scalability-Servers in der Basisinstallation

In der Basisinstallation kann der Scalability-Server folgende Tasks ausführen:

- Bereitstellen eines Registrierungsmechanismus für Agenten, die eine Verbindung herstellen.
- Empfangen eines von Agenten gepushten Basisinventars.
- Registrieren des Scalability-Servers bei einem Manager.
- Empfangen der vom Manager gepushten Konfiguration des Scalability-Servers.
- Weiterleiten von Agentenregistrierungs- und Basisinventarinformationen, die der Manager anfordert.
- Weiterleiten der vom Manager gepushten Agentenkonfigurationen.

Zusätzlich können produktspezifische Aufgaben für die Funktionalitäten Asset Management, Remote Control und Software Delivery (einschließlich der BS-Installationsverwaltung) aktiviert werden.

Für den einwandfreien Betrieb der Software Delivery (SD)-Funktionalität des Scalability-Servers wird mit jedem Scalability-Server ein SD-Agent installiert. Versuchen Sie nicht, den SD-Agenten vom Scalability-Server zu entfernen, da andernfalls Fehlfunktionen des Scalability-Servers auftreten können.

Außerdem muss der Agent des Scalability-Servers bei diesem Scalability-Server und keinem anderen registriert werden. Sie können dies prüfen, indem Sie auf dem Scalability-Server "caf setserveraddress" ausführen. Dies muss ergeben, dass "localhost" oder eine entsprechende Adresse auf den lokalen Host verweist. Wenn die zurückgegebene Adresse auf einen anderen Scalability-Server verweist, können Sie dies über den Befehl "caf setserveraddress localhost" auf dem entsprechenden Scalability-Server korrigieren.

Scalability-Server und Bereitstellung virtueller Anwendungen

Das Registrierungsassistent für Pakete mit virtuellen Anwendungen (den Sie verwenden, um Images der virtuellen Anwendung zu importieren und Pakete in der Softwarepaketbibliothek zu erstellen) erstellt die folgenden Softwarepakete für jedes Image der virtuellen Anwendung:

- Staging—Dieses Paket bietet Zugriff auf die virtuelle Anwendung für eigenständige und Streaming-Modi der Paketlieferung. Dieses Paket enthält das Image der virtuellen Anwendung.
- Eigenständig—Dieses Paket wird verwendet, um die virtuelle Anwendung lokal auf dem Zielcomputer zu installieren.
- Streaming—Dieses Paket wird verwendet, um die virtuelle Anwendung downstream von einem Streaming-Server zu erhalten und sie auf dem lokalen Computer auszuführen.

Sie stellen das Paket zur Bereitstellung der virtuellen Anwendung durch Staging auf dem Scalability-Server bereit. Der Scalability-Server fungiert auch als Streaming-Server für virtuelle Anwendungen. Darum werden Staging-Pakete für das Streaming virtueller Anwendungen auf die Zielcomputer auf dem Scalability-Server bereitgestellt.

Der Microsoft App-V-Streaming-Server verwendet zwei Protokolle für die Streaming-Kommunikation: RTSP (nicht gesichert) und RTSPS (gesichert). Standardprotokoll und -port für den Microsoft App-V-Streaming-Server sind RTSP und Port 554. Wenn Sie das gesicherte RTSPS-Protokoll mit Port 322 verwenden möchten, müssen Sie den Streaming-Server dementsprechend konfigurieren. Informationen zur Konfiguration des Microsoft App-V-Streaming-Servers finden Sie in der Dokumentation von Microsoft.

Sie stellen die eigenständigen und Streaming-Pakete vom Domänen-Manager auf den Zielcomputern bereit. Sie können auch Pakete vor der Bereitstellung auf Zielcomputern auf dem Scalability-Server zwischenspeichern. Sie können Standardbereitstellungsmethoden für Software Delivery verwenden, um Pakete mit virtuellen Anwendungen auf Zielcomputern bereitzustellen.

Hinweis: Weitere Informationen zum Packen und zur Bereitstellung virtueller Anwendungen finden Sie im *Software-Delivery-Administrationshandbuch*.

Aspekte der Boot-Server-Installation des BS-Installationsverwaltung

Der Boot-Server der BS-Installationsverwaltung (OSIM) wird als Teil eines Scalability-Servers installiert. Die Boot-Server-Installation stellt automatisch einen TFTP-Server (mit eingeschränkten Zugriffsrechten) und einen PXE-Server zur Verfügung.

Wenn Sie diese Funktionalität nicht nutzen möchten, können Sie den Boot-Server-Dienst während der Installation des Scalability-Servers oder danach über folgende CAF-Befehle deaktivieren:

```
caf stop sdmpcserver
```

```
caf disable sdmpcserver
```

Wenn Sie den Boot-Server-Dienst erneut aktivieren möchten, geben Sie die folgenden CAF-Befehle ein:

```
caf enable sdmpcserver
```

```
caf start sdmpcserver
```

Agent

Agenten sind auf allen verwalteten Endsystemen aller unterstützen Betriebsumgebungen vorhanden, auf denen die Agenten jeweils einzelne Tasks ausführen.

Wenn ein Agent beim ITCM-Manager registriert ist, dann ist die Host-UUID das Hauptattribut, das verwendet wird, um den Computer mit einem vorhandenen Computerdatensatz in der MDB abzugleichen. Wenn die Host-UUID keine Übereinstimmung hat, dann werden der Hostname und die MAC-Adressen verwendet, um den Computer abzugleichen.

Wenn eine Übereinstimmung mit dem Hostnamen und den MAC-Adressen gefunden wird, dann bedeutet dies, dass die Host-UUID des Computers geändert wurde. Zum Beispiel führt eine BS-Wiederinstallation zur Änderung der Host-UUID des jeweiligen Computers. Der Computerdatensatz wird dann mit der neuen Host-UUID aktualisiert, und der Software Delivery-Jobcontainer "Neuinstallation nach Absturz" (RAC) wird erstellt.

Wenn keine Übereinstimmung auf dem Hostnamen und den MAC-Adressen gefunden wird, dann wird ein neuer Computer erstellt, und der Jobcontainer "Neuinstallation nach Absturz" wird nicht erstellt.

In einigen Szenarien wird ein duplizierter Computer erstellt, statt einen vorhandenen Datensatz abzugleichen. Um diese Szenarien zu vermeiden, wurde der Übereinstimmungsalgorithmus auf dem Hostnamen und den MAC-Adressen verbessert. Vorher wurde nur die primäre MAC-Adresse verwendet, um die vorhandenen MAC-Adressen abzugleichen. Jetzt wird der vollständige Satz der normalen MAC-Adressen vom Computer in der Übereinstimmung verwendet. Die normalen MAC-Adressen schließen die vorübergehenden MAC-Adressen aus, zum Beispiel aus einem VPN, das zu falschen Übereinstimmungen führen könnte.

Die untere Tabelle fasst die Fälle zusammen, bei denen ein neuer Computer erstellt und ein vorhandener Computer abgeglichen wird, wenn eine Host-UUID, der Hostname oder die MAC-Adresse geändert wird.

Hinweis: Der in der Tabelle verwendete Bindestrich (-) zeigt an, dass das System die Suche nach Änderungen ignoriert.

Geänderte Host-UUID	Geänderter Hostname	Alle geänderten Stammgast-MACs	Geänderte primäre MAC	Erstelltes neues Asset	RAC
N	-	-	-	N	N
J	N	N	-	N	J
J	N	-	N	N	J
J	N	J	J	J	N
J	J	-	-	J	N

Hinweis: In einer Umgebung mit virtuellen Computern, z. B. XenServer, Hyper-V, ESX, muss der Administrator sicherstellen, dass jeder virtuelle Computer eine eindeutige MAC-Adresse innerhalb des Domänenbereichs hat.

Hinweis: Wenn ein Computer vorregistriert ist, sollte der Administrator sicherstellen, dass eine normale MAC-Adresse eingegeben wurde.

Konzept der Agentenpakete

Das Konzept der Agentenpakete (DSM-Agenten) in CA ITCM trennt die tatsächlichen Agentenfunktionen von einzelnen Sprachressourcen. Dieses Konzept bietet die folgenden Vorteile hinsichtlich der Agentenbereitstellung und -installation:

- **Sprachspezifische, nur für Agenten bestimmte Sprachpakete**

  Das Konzept der Agentenpakete ermöglicht Ihnen, Sprachpakete separat zu installieren. Ein Sprachpaket enthält alle Sprachressourcen für die Sprache, die für die Agenteninstallation erforderlich ist.

- **Erstellung eines einzigen Installationspakets mit ausschließlich erforderlichen Komponenten**

  Mit Hilfe des dsmPush-Skripts können Sie benutzerdefinierte individuelle Installationspakete erstellen, beispielsweise ein Paket mit Asset Management- und Software Delivery-Funktionalitäten sowie sechs Sprachpaketen.

Das Paketformat für Agenten ist eine Kombination aus Agentenfunktionen mit keinen oder mehreren Sprachpaketen. Bei fehlender Angabe eines Sprachpakets wird standardmäßig ENU (Englisch (USA)) verwendet. Die englischen Ressourcen sind stets als Teil der Agentenfunktionalität enthalten und sind daher auch nicht in einem eigenen Sprachpaket zu finden. Es ist jedoch möglich, ein eigenständiges Sprachpaket auf einem Agenten bereitzustellen.

Hinweis: Weitere Informationen zu Sprachpaketen finden Sie im Kapitel "Installation von CA ITCM" unter "Ändern der Produktsprache nach der Installation".

Der DSM-Agent kann über die folgenden Plug-ins verfügen:

- CA DSM Agent + Software Delivery-Plug-in (SD-Agent)
- CA DSM Agent + Remote Control-Plug-in (RC-Agent)
- CA DSM Agent + Asset Management-Plug-in (AM-Agent)
- CA DSM Agent + Basic Inventory-Plug-in (BHI-Agent)
- Software Delivery-Katalog (SD-Katalog)
- Remote Control-Viewer (RC-Viewer)
- Alle von Agentenseite abhängigen Komponenten, z. B. DTS (Data Transport Service)

Agentenkonfiguration

Agenten werden von ihrem Domänen-Manager zentral verwaltet und konfiguriert. Diese Tasks werden über den DSM-Explorer ausgeführt.

Remote Control-Viewer

Der Remote Control-Viewer (RC Viewer) ist die Benutzeroberfläche, die Zugriff auf die Remote Control-Dienste bietet. Nach der Installation können Sie über die DSM-Explorer-Baumstruktur oder die Befehlszeile auf den RC Viewer zugreifen.

Die Remote Control-Funktionalität unterstützt einen Win32- oder Webbrowser-Client. Der Browser-Client setzt Microsoft Internet Explorer 6.0 voraus.

Zu den charakteristischen Merkmalen des RC Viewers gehören:

Remote Control

Hiermit wird der Eindruck vermittelt, als säßen Sie direkt vor dem Computer, den Sie steuern.

Dateiübertragung

Überträgt Dateien zwischen Viewer und Host-Computern.

Chat

Stellt während einer Remote Control-Sitzung eine interaktive Chat-Sitzung mit einem Benutzer her.

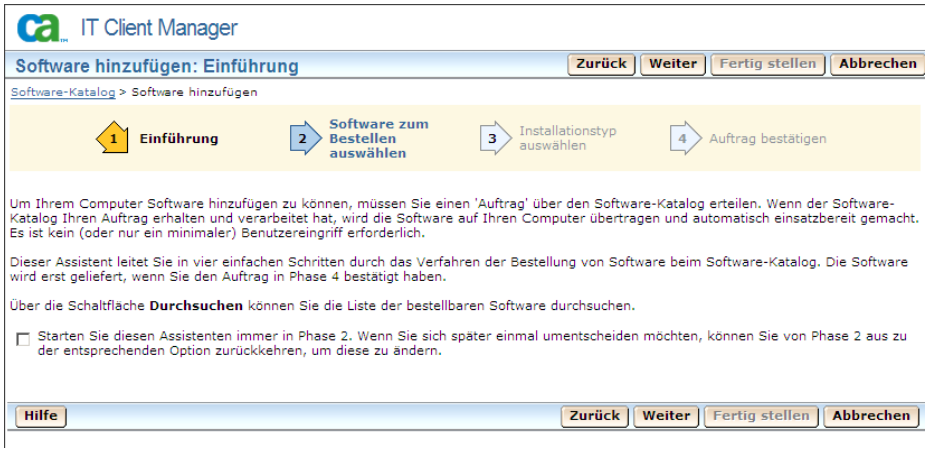
Sitzungsaufzeichnung

Aufzeichnen der Starts und Stopps der Remote Control-Sitzung.

Softwarekatalog

Der Softwarekatalog (auch als Software Delivery-Katalog oder SD-Katalog bezeichnet) ist ein Agenten-Plug-in, das Ihnen "Self-Service" ermöglicht. Über die assistentengestützte Oberfläche des Softwarekatalogs können Sie auf Ihrem Computer Software aus einer vom Administrator bereitgestellten Bibliothek installieren oder entfernen.

Der folgende Screenshot zeigt die Einführungsseite des Assistenten zum Hinzufügen von Software:


IT Client Manager
Software hinzufügen: Einführung
Zurück
Weiter
Fertig stellen
Abbrechen
Software-Katalog > Software hinzufügen
1 Einführung
2 Software zum Bestellen auswählen
3 Installationstyp auswählen
4 Auftrag bestätigen
Um Ihrem Computer Software hinzufügen zu können, müssen Sie einen 'Auftrag' über den Software-Katalog erteilen. Wenn der Software-Katalog Ihren Auftrag erhalten und verarbeitet hat, wird die Software auf Ihren Computer übertragen und automatisch einsatzbereit gemacht. Es ist kein (oder nur ein minimaler) Benutzereingriff erforderlich.
Dieser Assistent leitet Sie in vier einfachen Schritten durch das Verfahren der Bestellung von Software beim Software-Katalog. Die Software wird erst geliefert, wenn Sie den Auftrag in Phase 4 bestätigt haben.
Über die Schaltfläche Durchsuchen können Sie die Liste der bestellbaren Software durchsuchen.
Starten Sie diesen Assistenten immer in Phase 2. Wenn Sie sich später einmal umentscheiden möchten, können Sie von Phase 2 aus zu der entsprechenden Option zurückkehren, um diese zu ändern.
Hilfe
Zurück
Weiter
Fertig stellen
Abbrechen

Der folgende Screenshot zeigt ein Beispiel für die Seite "Software zum Bestellen auswählen" des Assistenten zum Hinzufügen von Software:

AM Remote-Agent

CA ITCM unterstützt die Virtualisierung der Plattform, einschließlich der folgenden virtualisierten UNIX-Umgebungen:

- HP nPartitions und virtuelle Partitionen
- HP Integrity Virtual Machines
- Logische IBM-Partitionen
- SUN Dynamic System Domains
- SUN Dynamic System Domains auf Sun SPARC Enterprise M-Series-Servern
- Virtuelle Computer, die unter VMware ESXi ausgeführt wird.
- Virtuelle Computer, die unter Citrix XenServer ausgeführt werden.

Der AM Remote-Agent ersetzt den r12-partitionierten UNIX-Server. Seine Funktionalität wurde jedoch vollständig in den AM Remote-Agenten integriert. Dieser Agent wird ausschließlich im DSM-Explorer konfiguriert, um Information für virtuelle Hosts zu erfassen.

Hinweis: Detaillierte Informationen über den AM Remote-Agenten finden Sie im *Asset Management-Administrationshandbuch*. Die aktuelle Liste unterstützter Plattformen, finden Sie in der Kompatibilitätsmatrix.

DSM Reporter

Der DSM-Reporter ist ein Abfrage-Tool, mit dem Informationen aus der Datenbank extrahiert werden.

Berichte können kurzfristig oder nach Plan erzeugt werden. Der DSM-Reporter erhöht den Wert der CA ITCM-Daten durch Organisieren, Filtern und Darstellen der Daten. Mit dem DSM-Reporter können Sie auch Daten in CSV- oder HTML-Dateien (*.csv bzw. *.html) exportieren. Die Dateien können anschließend in Tabellenkalkulationen, Tools für die Budgetplanung u. A. eingelesen werden.

Der DSM-Reporter ist dem DSM-Explorer in Aussehen und Verhalten ähnlich. Drag-and-Drop-Optionen zum Drucken von CA ITCM-Einheiten und -Gruppen sowie zum Erstellen neuer Berichte auf der Grundlage von Abfragen erweitern die Funktionalität des DSM-Reporters als Erweiterung des DSM-Explorers.

Hinweis: Stellen Sie beim ersten Start des DSM Reporter nach der Installation sicher, dass Sie genügend Zeit für den Import aller Berichtsvorlagen in die Datenbank lassen. Sollten beim Import der Berichtsvorlagen Probleme auftreten, können Sie als Umgehungslösung den Registrierungs-Editor öffnen und den Unterschlüssel in HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Unicenter ITRM\Reporter\Library löschen. Starten Sie den DSM Reporter nach der Löschung des Unterschlüssels erneut.

Unterstützte Betriebsumgebungen

CA IT Client Manager (CA ITCM) unterstützt alle wichtigen Betriebsumgebungen. Die aktuelle Liste unterstützter Betriebssystemplattformen finden Sie in der Kompatibilitätsmatrix.

Hinweis: In diesem Dokument verweist der Begriff UNIX auf die UNIX-Derivate AIX, HP-UX, Solaris und Mac-OS-X. Wenn eine Systemkomponente oder Softwarefunktion dieser Version nicht für alle UNIX-Derivate gilt, wird dies in der Beschreibung der Komponente oder Funktion angegeben.

Common Application Framework

Jede DSM-Komponente verwendet das Common Application Framework (CAF). CAF ist ein plattformübergreifender Dienstcontroller, der eine zentrale Steuerungsstelle für alle DSM-Komponenten ist.

CAF bietet DSM-Dienste dynamisch nach Bedarf mit Hilfe eines erweiterbaren Plug-in-Modells an. Jedes CAF-Plug-in ist ein Programm, das die Funktionalität von Agenten, Scalability-Servern oder Managern bietet. Ein CAF-Plug-in kann auch eine Erweiterung von CAF sein und einen allgemeinen Dienst bereitstellen, z. B. die Registrierung bei Scalability-Servern oder die Erkennung von Systemereignissen.

Üblicherweise startet CAF alle Plug-ins zur Boot-Zeit automatisch. CAF kann Plug-ins auch auf Anforderung über die Befehlszeile und mit Hilfe seines Zeitplans zu bestimmten Zeiten und in regelmäßigen Intervallen starten und beenden. Eine Beschreibung, wie geplante Jobs zum Ausführen in CAF angegeben werden, finden Sie im Anhang "Mit CAF geplante Jobs" (siehe Seite 605).

CAF kann auch Plug-ins auf Statusinformationen abfragen und Meldungen von anderen Plug-ins weiterleiten.

Wichtig! Unter Windows wird CAF standardmäßig so installiert, dass es sich als lokales Systemkonto anmeldet. Wenn Sie diese Netlogon-Eigenschaft aus Sicherheitsgründen ändern, muss dies nach der Installation über die Windows-Systemsteuerung unter "Computerverwaltung", "Dienste" erfolgen. Wenn Sie jedoch zu einem Konto mit eingeschränkten Berechtigungen wechseln, kann dies zu unerwartetem Verhalten oder verringertem Funktionsumfang von CA IT Client Manager führen.

Benutzeroberfläche des Application Frameworks

Normalerweise erübrigt sich eine Interaktion mit dem Application Framework (CAF), da es als Dienst im Hintergrund ausgeführt wird. CAF bietet jedoch eine Befehlszeilenschnittstelle (Befehl "caf"), über die Administratoren alle CAF-Funktionen lokal oder per Remote-Zugriff aufrufen können, wie in den folgenden Beispielen dargestellt:

- Abfragen des aktuellen Status aller CAF-Plug-ins
- Starten und Beenden von CAF und allen zugeordneten Plug-ins und Prozessen.
- Starten, Beenden und Abfragen des Status eines einzelnen Plug-ins.
- Aktivieren und Deaktivieren von Plug-ins.

In den meisten Fällen weist die CAF-Befehlszeilenschnittstelle CAF in einer Meldung an, den Befehl auszuführen. Ausnahmen sind die Befehle zum Starten und Beenden des CAF-Dienstes oder des Daemons selbst und einige Konfigurationsbefehle.

Hinweis: Unter Windows Vista werden für die meisten caf-Befehle volle Administratorrechte benötigt. Wenn Sie Mitglied der Administratorgruppe sind, jedoch als ein anderer Benutzer angemeldet sind, wird das Befehlszeilenfenster normalerweise mit Benutzerrechten ausgeführt. Um caf-Befehle verwenden zu können, müssen Sie das Befehlszeilenfenster durch Klicken mit der linken Maustaste auf das entsprechende Symbol und Auswahl von "Als Administrator ausführen" öffnen.

Taskleiste

Die Taskleiste ist ein Tool, mit dem Benutzer Zugriff auf Systemdienste erhalten, z. B. auf das Common Application Framework (CAF).

Der Infobereich wird als Symbol in der Taskleiste auf dem Desktop aller Betriebssysteme außer UNIX angezeigt. Wenn Sie mit der rechten Maustaste auf das Symbol klicken, können Sie einen der im Kontextmenü verfügbaren Dienste auswählen. Wenn es erforderlich ist, fordert die Taskleistenfunktion vor dem Start des Dienstes eine Interaktion des Benutzers an.

Die über die Taskleiste verfügbaren Dienste und die Anzeige des Taskleistensymbols (ein- oder ausblenden) werden in der Konfigurationsrichtlinie festgelegt.

Während der Laufzeit von CA ITCM können Sie die Taskleiste und ihr Symbol mit folgenden Befehlen über die Befehlszeile steuern:

cfSysTray

Startet den Infobereich, wenn sein Status in der Konfigurationsrichtlinie auf "Anzeigen" festgelegt ist. Das Symbol wird in der Taskleiste angezeigt.

cfSysTray show

Startet den Infobereich (wenn er noch nicht gestartet wurde) und legt seinen Status in der Konfigurationsrichtlinie auf "Anzeigen" fest. Das Symbol wird in der Taskleiste angezeigt.

cfSysTray stop

Beendet die Taskleiste. Das Taskleistensymbol wird in der Taskleiste ausgeblendet.

cfSysTray hide

Beendet den Infobereich und legt seinen Status in der Konfigurationsrichtlinie auf "Ausblenden" fest. Das Taskleistensymbol wird in der Taskleiste ausgeblendet.

Für die CA ITCM-Taskleiste muss unter Linux das GIMP-Toolkit GTK+ 1.2 (oder höher) installiert sein. Das GTK ist nicht im Lieferumfang von CA ITCM enthalten. Sie müssen die erforderliche Version unter www.gtk.org herunterladen.

Protokollierung

Die Common Component Library (CCL) unterstützt umfassende Tracing-Funktionen und verfügt über einen Absturz-Handler, der die Diagnose schwerwiegender Fehler unterstützt. Diese Dienste stehen auch den meisten Plug-in-Komponenten zur Verfügung und werden von ihnen genutzt.

Die Common Application Framework-Dienste (CAF) protokollieren ihre Aktivitäten in Protokolldateien. Der Grad der Detaildarstellungen hängt von der Trace-Ebene ab, die benutzerdefinierbar ist. Die Protokolldateien unterstützen Sie bei der Analyse von Problemen.

Standardmäßig wird die Trace-Ebene auf ERROR (Fehler) gesetzt. Wenn Sie weitere Trace-Informationen benötigen, können Sie die Trace-Ebene festlegen, z. B. können Sie sie für die Software Delivery-Funktionen oder Data Transport Service auf DETAIL festlegen, indem Sie *einen* der folgenden"cftrace"-Befehle ausführen:

```
cftrace -c set -f USD -l DETAIL -s 30000
```

```
cftrace -c set -f DTS -l DETAIL -s 30000
```

Mit der Option "-s" wird die Größe der Protokolldatei auf 30.000 KB festgelegt. Die Standardgröße beträgt 2.000 KB, was für die Trace-Ebene DETAIL u. U. zu klein ist. (Diese Trace-Datei wird überschrieben, wenn die Größenbeschränkung und die Anzahl der konfigurierten Trace-Dateien erreicht wurde.)

Unter Windows befinden sich die Protokolldateien aller CAF-Dienste unter "*Installationsverzeichnis*\logs" (Standard: C:\Programme\CA\DSM\logs).

Die während der Installation von CA IT Client Manager erstellten Protokolldateien befinden sich im temporären Ordner des jeweiligen Benutzers. Normalerweise verweist die Umgebungsvariable "%temp%" auf diesen Ordner.

Unter Linux befinden sich die Protokolldateien der CAF-Dienste unter "$CA_ITRM_BASEDIR/logs".

Die während der Installation von CA IT Client Manager erstellten Protokolldateien befinden sich unter "/opt/CA/installer/log".

Trace-Protokolldateien

CA ITCM-Komponenten erzeugen Trace-Protokolldateien ihrer Systemaktivitäten, während sie ausgeführt werden. Sie können diese Protokolldateien verwenden, um Probleme zu analysieren und zu beheben, die auftreten können.

Jeder CA ITCM-Prozess schreibt in seine eigene Trace-Protokolldatei. Wenn Comstore eine Trace-Konfiguration für einen Prozess enthält, schreibt der Prozess seine Trace-Informationen in die definierte Datei. Wenn Comstore keine Trace-Konfiguration für einen Prozess enthält, schreibt der Prozess seine Trace-Informationen in eine Datei, die nach dem Namen des Prozesses benannt wird. Wenn es mehrere Instanzen des gleichen Prozesses gibt, können Sie festlegen, dass jede Instanz in Ihr eigenes eindeutig benanntes Trace-Protokoll schreibt. Diese Funktion ist allerdings standardmäßig abgestellt, um die Erstellung zahlreicher Trace-Dateien zu verhindern. Sie können diese Funktion einschalten (durch die normale Konfiguration), wenn Sie Systemprobleme beheben möchten.

Wenn die Trace-Ebene für einen Prozess auf FEHLER festgelegt ist und eine Trace auf FEHLER-Ebene erhoben wird, schreibt CA ITCM zusätzliche Trace-Informationen auf INFO-Ebene in die Trace-Protokolldatei. Diese zusätzlichen Informationen auf INFO-Ebene bieten Ihnen mehr Daten über den Zusammenhang, in dem der Fehler aufgetreten ist, indem sie die Traces niedrigerer Ebenen angeben, die zum Fehler geführt haben.

Sie können die Parameter festlegen, die die Tracing-Funktion durch die Ccnfcmda-Befehlszeile steuern.

Hinweis: Für ausführlichere Information über den Ccnfcmda-Befehl zur Agentenkonfiguration tippen Sie "<command> /?" in der Befehlszeile eingeben.

Das Diagnose-Tool "dsminfo"

CA Technologies stellt das Tool "dsmInfo" zur Verfügung, das Diagnoseinformationen von Systemen erfasst, in denen CA ITCM installiert ist. Die gesammelten Daten werden in eine einzelne Datei komprimiert, die Protokolldateien, Systeminformationen, Verzeichnisstrukturen sowie Registrierungs- und Umgebungsinformationen enthält. Dieses Diagnose-Tool ist befindet sich auf dem CA ITCM Produktinstallationsdatenträger im Ordner "DiagnosticTools".

Wenn Sie ein Problem mit CA ITCM reproduzieren können, führen Sie den folgenden Befehl aus, um die Trace-Ebene in DETAIL zu ändern:

```
cftrace -c set -l DETAIL
```

Reproduzieren Sie das Problem und sammeln Sie die Diagnoseinformationen mit dem Tool "dsmInfo".

Hinweise:

Weitere Information zu diesem Tool finden Sie in der Datei DSMInfoReadMe.txt im Ordner "DiagnosticTools" auf dem Datenträger für die Produktinstallation.

Das Tool "dsmInfo" erzeugt standardmäßig ".7z"-Dateien . Diese Dateien bieten bessere Verdichtung als ZIP-Dateien, so ist es leichter, sie nach CA Technologies hochzuladen.

Allgemeine Konfiguration

CA ITCM wird zentral über eine allgemeine Konfigurationskomponente konfiguriert. Die allgemeine Konfigurationskomponente bietet Funktionen zum Zugreifen auf die Konfigurationsdaten von CA ITCM sowie für deren Speicherung und Verwaltung.

Konfigurationsparameter

Die kleinste Einheit einer Konfiguration ist ein Parameter. Parameter können in Konfigurationsrichtlinien gruppiert werden, die Sie Computern oder Computergruppen zuweisen können.

Im Konfigurationsmodell werden folgende Objekte definiert:

Parameter

Enthält Konfigurationsdaten. Ein Parameter hat einen Namen und enthält mindestens einen Wert.

Parameterinformationen

Enthalten zusätzliche Informationen zu einem Parameter.

Parameterabschnitt

Eine Zusammenstellung von Parametern, die logisch zusammengehören. Sie konfigurieren beispielsweise bestimmte, einander entsprechende Funktionen. Mit Parameterabschnitten wird die hierarchische Struktur von Parametersätzen hergestellt.

Konfigurationsrichtlinie

Eine Zusammenstellung gruppenspezifischer oder computerspezifischer Parameter.

Konfiguration

Stellt den Konfigurationsstatus eines Computers oder einer Computergruppe dar und ist ihnen zugewiesen. Der Wert einer Konfiguration kann geplant, zeitlich geplant, aktiv oder ein Fehler sein.

Verwaltung von Konfigurationsparametern

Die Standardrichtlinie, d. h. der festgelegte Standardparameter, des Managers enthält Parameter für das Remote-Management. Die Standardrichtlinie enthält keine Parameter, die nur für lokale Anwendungen Bedeutung haben, die auf dem lokalen Computer ausgeführt werden.

Die Standardrichtlinie enthält zwei Typen von Verwaltungsmodi: lokal verwaltet oder zentral verwaltet. Der Verwaltungsmodus eines Parameters kann nur im Manager geändert werden.

- Lokal verwaltete Parameter werden von Anwendungen gesteuert, die auf dem lokalen Computer ausgeführt werden.
- Zentral verwaltete Parameter werden von Richtlinien des Managers gesteuert. Lokale Anwendungen haben nur Lesezugriff auf diese Parameter. Zentral verwaltete Parameter haben Vorrang gegenüber lokal verwalteten Parametern.

Einige Anwendungen, beispielsweise Remote Control, können in einem eigenständigen Modus installiert werden. Bei eigenständigen Installationen werden die Konfigurationsparameter nicht von der Standardrichtlinie des Managers gesteuert. Auch werden die Parameterwerte nicht an den Manager gemeldet. Der eigenständige Modus hat Vorrang gegenüber dem lokal und zentral verwalteten Modus. Der eigenständige Modus wird während der Installation der Anwendung (beispielsweise Remote Control) eingerichtet.

Konfigurationsrichtlinien

Sie können Parameter zu Verwaltungszwecken in Konfigurationsrichtlinien zusammenfassen. Diese Richtlinien können Computern oder Computergruppen zugewiesen werden.

Ein einzelner Computer oder eine einzelne Gruppe kann auch mehreren Konfigurationsrichtlinien unterliegen. In diesem Fall können sich die Parametereinstellungen, die in einer Richtlinie festgelegt sind, mit den Parametereinstellungen einer anderen Richtlinie überschneiden. Zum Lösen von Konflikten müssen Sie folgende Regeln einhalten, wenn sich Konfigurationsrichtlinien überschneiden:

- Richtlinien, die einer Gruppe zugewiesen sind, werden von den untergeordneten Objekten der Gruppe geerbt. Ein untergeordnetes Objekt kann eine Gruppe oder ein Computer sein.
- In einer Hierarchie setzen auf der untergeordneten Ebene zugewiesene Richtlinien die Richtlinien auf der übergeordneten Ebene außer Kraft. D. h., dass alle auf der übergeordneten Ebene festgelegten Parameter auch für das untergeordnete Objekt festgelegt werden. Wenn aber eine untergeordnete Richtlinie und eine übergeordnete Richtlinie sich überschneiden, hat die untergeordnete Richtlinie Vorrang.

Konfigurationsbericht von Agenten

Wenn die Parametereinstellungen eines Agenten geändert werden, meldet er diese Änderungen immer seinem Manager. Auf dem Manager können diese Einstellungen im DSM-Explorer als "Gemeldete Konfiguration" angezeigt werden.

Konfiguration des Enterprise-Manager-Agenten

Die CA IT Client Manager-Infrastruktur verwendet eine allgemeine Konfigurationsarchitektur und -methodologie. Administratoren können mit der DSM-Explorer-Oberfläche Änderungen an der Konfigurationsrichtlinie vornehmen. Diese Änderungen werden von einem DSM-Domänen-Manager in der Management-Datenbank (MDB) gespeichert. Anschließend werden die Änderungen an einen Agenten übermittelt, der sie anwendet.

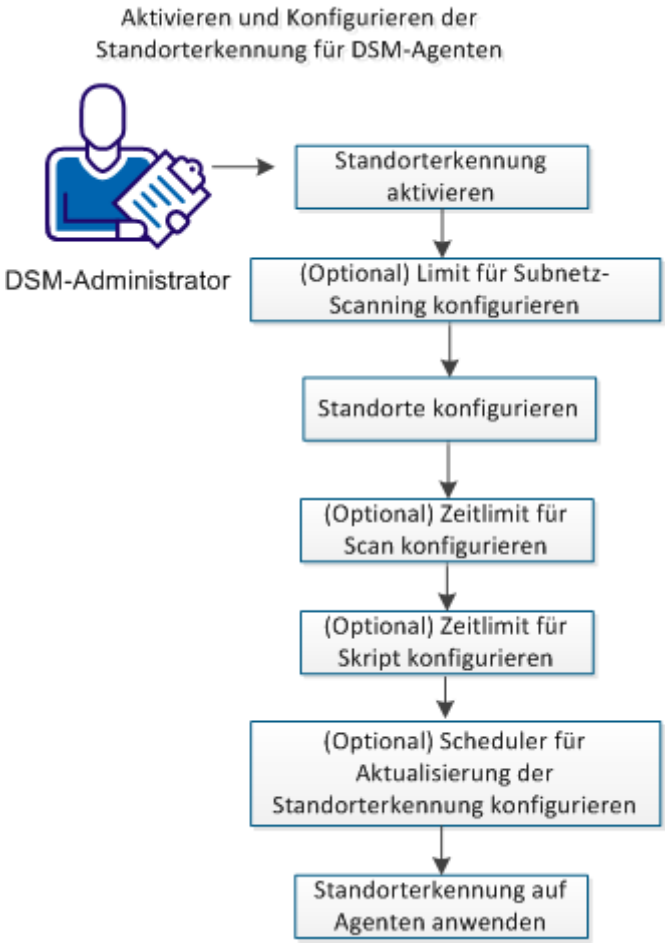
Mit Ausnahme eines Einzelfalles ist dies eine einfache Lösung. In Fällen, in denen jedoch ein Enterprise-Manager vorhanden ist, wird die Architektur des Konfigurationsmanagement etwas weniger intuitiv gestaltet.

Um eine verwaltete Konfiguration zu unterstützen, muss ein Enterprise-Manager selbst verwaltet werden. Dies erfordert die Installation eines Agenten. Agenten kommunizieren mit Scalability-Servern, die dann wiederum mit Domänen-Managern kommunizieren. Sie müssen also entscheiden, welche Scalability-Server und Domänen-Manager den Enterprise-Manager-Computer verwalten.

In den meisten Organisationen wird nur ein einzelner Enterprise-Manager bereitgestellt.

So aktivieren und konfigurieren Sie Standorterkennung

Als Administrator umfasst Ihre Verantwortung das Erstellen einer Richtlinie zur Standorterkennung. Sie können den Computer so konfigurieren, dass eine Berichterstellung an einen entsprechenden Scalability-Server erfolgt, wenn eine Änderung in Speicherort entdeckt wird. Sie können die Funktion der Standorterkennung auf eine Richtlinie auf den DSM-Agenten anwenden, um es dem Computer zu ermöglichen, die Regeln zur Standorterkennung auszuwerten.


Aktivieren und Konfigurieren der Standorterkennung für DSM-Agenten
DSM-Administrator
Standorterkennung aktivieren
(Optional) Limit für Subnetz-Scanning konfigurieren
Standorte konfigurieren
(Optional) Zeitlimit für Scan konfigurieren
(Optional) Zeitlimit für Skript konfigurieren
(Optional) Scheduler für Aktualisierung der Standorterkennung konfigurieren
Standorterkennung auf Agenten anwenden

Gehen Sie folgendermaßen vor:

1. Aktivieren Sie die Standorterkennung (siehe Seite 58).
2. (Optional) Konfigurieren Sie das Limit für Subnetz-Scanning (siehe Seite 59).
3. Konfigurieren Sie die Standorte (siehe Seite 60).
4. (Optional) Konfigurieren Sie das Zeitlimit für Scan (siehe Seite 67).
5. (Optional) Konfigurieren Sie das Skript-Zeitlimit (siehe Seite 67).
6. (Optional) Konfigurieren Sie den Scheduler für "Standorterkennung aktualisieren" (siehe Seite 68).
7. Wenden Sie die Standorterkennung auf Agenten an (siehe Seite 70).

Aktivieren der Standorterkennung

Die Funktion zur Standorterkennung ist entweder für eine Neuinstallation oder für ein Upgrade nicht standardmäßig aktiviert. Durch das Aktivieren der Richtlinie zur Standorterkennung können Sie Änderungen am geografischen Standort eines Agenten erkennen. Wenn eine Änderung erkannt wird, wertet der Agent die Regeln aus und stellt dann eine Verbindung mit einem entsprechenden Scalability-Server her.

Wichtig! Bevor Sie die Funktion zur Standorterkennung aktivieren, deaktivieren Sie andere Lösungen zur Standorterkennung, die sich in der ITCM-Umgebung befinden.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "DSM", "Agent", "Common Agent", "Allgemein", "Standorterkennung".

   Folgende Parameter der Standorterkennung werden angezeigt.

   - Aktiviert
   - Limit für Subnetz-Scanning
   - Speicherorte
   - Zeitlimit für Scan
   - Skript-Zeitlimit

2. Wählen Sie "Aktiviert" aus, und klicken Sie dann im Portlet "Tasks" auf "Eigenschaften der Einstellung".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

3. Wählen Sie "Wahr" aus dem Feld "Wert" aus, klicken Sie dann auf "OK".

   Die Funktion wird in der Richtlinie aktiviert. Die Richtlinie wird erst dann aktiv, wenn Sie sie versiegelt und auf einen Agenten angewendet haben.

Hinweis:

- Wenn der Agent auf dem gleichen Computer wie ein Scalability-Server ausgeführt wird, dann ist die Richtlinie zur Standorterkennung immer deaktiviert.
- Wenn der Agent-Scalability-Server als zentral verwaltet markiert ist, kann die Funktion zur Standorterkennung des Agenten nach der Regelauswertung den Wert nicht ändern.

(Optional) Konfigurieren des Limits für Subnetz-Scanning

Sie können das Limit für Subnetz-Scanning konfigurieren, um das Scanning des Subnetzes zur Suche der Scalability-Server in anderen Domänen zu erlauben oder zu verhindern.

Gehen Sie wie folgt vor:

1. Navigieren Sie zur Konfigurationsrichtlinie zur Standorterkennung.

   Die Parameter der Standorterkennung werden im rechten Bereich angezeigt.
2. Doppelklicken Sie auf "Limit für Subnetz-Scanning".
3. Klicken Sie im Portlet "Tasks" auf "Eigenschaften der Einstellung".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.
4. Ändern Sie das Feld "Wert" entsprechend für Ihre Umgebung.

   Standard: True
5. Klicken Sie auf "OK".

   Der Parameter "Limit für Subnetz-Scanning" ist konfiguriert.

Konfigurieren von Standorten

Definieren Sie die Standortregeln, um Änderungen an geografischen Standorten zu unterstützen und um es Agenten zu ermöglichen, eine Verbindung zu den entsprechenden Scalability-Servern herzustellen. Die Agenten werten die von Ihnen erstellten Regeln aus, um zu bestimmen, welche Scalability-Server verbunden werden sollen.

Gehen Sie wie folgt vor:

1. Wählen Sie "Standorte" aus, und klicken Sie dann im Portlet "Tasks" auf "Eigenschaften der Einstellung".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

2. Klicken Sie auf "Zeile hinzufügen", um die Regeln zu konfigurieren.

   Die Funktion fügt der aktuellen Tabellenstruktur eine Zeile mit folgenden Parametern hinzu:

   - Positionsname
   - Priorität
   - Adressbereich
   - Scalability-Server
   - Subnetz-Scanning
   - Skript

3. Konfigurieren Sie jeden Parameter, und klicken Sie dann auf "OK".

   Die Parametereinstellungen der Standorte sind konfiguriert.

Wichtig! Über die Funktion wird der Adressbereich nicht vollständig überprüft oder die Werte für "Servername", "Subnetz-Scanning" und "Skript" werden nicht validiert. Gehen Sie beim Festlegen dieser Parameter sorgfältig vor.

Konfigurieren der Priorität für Standortregeln

Sie können die Priorität angeben, mit der die Funktion auswählt, welche Standortregeln bearbeitet werden sollen. Der Agent wertet die Regeln aus und verwendet die angegebene Priorität, um zu bestimmen, welche Regel angewendet werden soll.

Zum Beispiel erstellen Sie zwei Regeln (Regel "A" und Regel "B"). Gehen wir davon aus, dass Sie Regel "A" mit Priorität 1 und Regel "B" mit Priorität 2 konfigurieren. Wenn Sie alle anderen Parameter mit den gleichen Werten für Regel "A" und Regel "B" konfigurieren, dann findet der Agent zwei Übereinstimmungen. Allerdings wird Regel "A" angewendet, da Regel "A" die höhere Priorität hat.

Gehen Sie wie folgt vor:

1. Doppelklicken Sie auf den neuen Wert unter "Priorität".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

2. Geben Sie die Priorität für die Standortregel im Feld "Wert" an, und klicken Sie dann auf "OK".

   Höchste Priorität: 0

   Niedrigste Priorität: 99999

   Die Priorität der Standortregel ist konfiguriert.

Konfigurieren des Adressbereichs für Standortregeln

Wenn die Agent-Adresse mit den Kriterien des IP-Adressbereichs übereinstimmt, dann wird die Standortregel in die Auswahl eingeschlossen. Die Funktion zur Standorterkennung unterstützt sowohl IPv4-Adressen als auch IPv6-Adressen. Wenn der Agent mit mehreren Regeln übereinstimmt, verwendet die Funktion den Prioritätswert der Regeln, um zu bestimmen, welcher Server verwendet werden soll.

Gehen Sie wie folgt vor:

1. Doppelklicken Sie auf den neuen Wert in der Adressbereichsspalte.

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

2. Geben Sie den Adressbereich in das Feld "Wert" ein, und klicken Sie dann auf "OK".

   Beschränkungen: Der Minimalwert ist 1 Zeichen.

   Wenn Sie "IPv4" verwenden, können Sie die IP-Adresse, den IP-Platzhalter oder den IP-Bereich in der Adressbereichsspalte angeben. Beispiel:

   - **IP-Adressformat:** 192.168.1.1
   - **IP-Platzhalterformat:** 192.168.1.*
   - **IP-Bereichsformat:** 192.168.2.1-192.168.2.100

   Wenn Sie "IPv6" verwenden, können Sie verschiedene IPv6-Adresspräfixe in der Adressbereichsspalte angeben. Beispiel:

   2001:DB8::/48

   Identifiziert die Organisation, den Standort, den Unterstandort und das Subnetz. 48 ist die Länge des Präfixes in Bits, und die größtmögliche zulässige Bitanzahl ist 64.

   Besondere Adresspräfixe:

   FE80::/64

   Wird verwendet, um ein link-lokales Präfix, d. h. ein lokales Subnetz, abzugleichen.

   FEC0::/64

   Wird verwendet, um ein standortlokales Präfix abzugleichen.

   ::/0

   Wird verwendet, um alle IPv6-Adressen abzugleichen.

   Multicast-Gruppenadressen:

   FF02::1

   Wird verwendet, um alle Knoten auf dem lokalen Netzwerksegment abzugleichen (Link-lokal).

   FF05::1

Wird verwendet, um alle Knoten auf dem Standortnetzwerk abzugleichen (Standortlokal).

FF08::1

Wird verwendet, um alle Knoten auf dem Organisationsnetzwerk abzugleichen (Organisationslokal).

Der Adressbereich der Standortregel ist konfiguriert.

Konfigurieren des Scalability-Servers für Standortregeln

Die Spaltenwerte für "Scalability-Server", die Sie angeben können, definieren die IP-Adresse oder den FQDN (vollqualifizierter Domänenname) eines Scalability-Servers für den Agenten, zu dem mithilfe der Spalte "Scalability-Server" eine Verbindung hergestellt werden soll.

Gehen Sie wie folgt vor:

1. Doppelklicken Sie auf den neuen Wert unter "Scalability-Server".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

2. Geben Sie die IP-Adresse oder den FQDN des Scalability-Servers ein, mit dem der Agent, der sich im Adressbereich befindet, eine Verbindung herstellt.

   Der Scalability-Server der Standortregel ist konfiguriert.

Hinweis: Wenn Sie den Scalability-Server angeben, lassen Sie die Spalten "Subnetz-Scanning" und "Skript" leer. Wenn Sie den Scalability-Server nicht verwenden, lassen Sie die Spalte "Scalability-Server" leer.

Konfigurieren des Subnetz-Scanning für Standortregeln

Die Konfiguration für Subnetz-Scanning definiert die Regel für den Scan des angegebenen Subnetzes und entdeckt aktive Scalability-Server auf diesem Subnetz. Der Agent wertet dann die anderen Regeln und die geschätzten Antwortzeiten der aktiven Server aus, um den besten Server auszuwählen. Die Funktion zur Standorterkennung unterstützt sowohl IPv4-Adressen als auch IPv6-Adressen.

Gehen Sie wie folgt vor:

1. Doppelklicken Sie auf den neuen Wert in der Spalte "Subnetz-Scanning".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

2. Geben Sie das Subnetz-Scanning in das Feld "Wert" ein, und klicken Sie dann auf "OK".

   Wenn Sie "IPv4" verwenden, können Sie die IP-Adresse, den IP-Platzhalter oder den IP-Bereich in der Spalte "Subnetz-Scanning" angeben.

   Wenn Sie "IPv6" verwenden, können Sie verschiedene IPv6-Adresspräfixe in der Spalte "Subnetz-Scanning" angeben.

   Der Subnetz-Scan für die Standortregel ist konfiguriert.

Hinweis: Wenn Sie das Subnetz-Scanning angeben, lassen Sie die Spalten "Scalability-Server" und "Skript" leer. Wenn Sie das Subnetz-Scanning nicht verwenden, lassen Sie die Spalte "Subnetz-Scanning" leer.

Konfigurieren des Skripts für Standortregeln

Sie können ein Skript hinzufügen, das auf dem Agenten ausgeführt werden soll, und Sie können festlegen, welcher Scalability-Server verwendet werden soll. Zu Ihrer Verantwortung gehört, dem Agent-Computer das Skript bereitzustellen.

Gehen Sie wie folgt vor:

1. Doppelklicken Sie auf den neuen Wert in der Spalte "Skript".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

2. Geben Sie im Feld "Wert" den Namen des DM-Skripts an, und klicken Sie dann auf "OK".

   Hinweis: Sie können den Skriptspeicherort als absoluten Pfad oder als relativen Pfad angeben. Ein relativer Pfad bezieht sich auf das ITCM-Installationsverzeichnis, das sich normalerweise in einem der folgenden Speicherorte befindet:

   Windows:

   C:\Program Files(x86)\CA\DSM

   Unix, Linux:

   /opt/CA/DSM

   Die Funktion übergibt folgende Parameter an das Skript zur Serverauswahl:

   -o <Name der Ausgabedatei>

   Benennt die Datei, in der das Skript den Namen des Scalability-Servers, der identifiziert wird, schreibt.

   -x <Name der Fehlerdatei>

   Benennt die Datei, in der das Skript alle generierten Fehlerinformationen schreibt.

   -a <Übereinstimmende Adresse>

   Identifiziert die Adresse, die übereinstimmt und zur Ausführung dieses Skripts führt.

   Das DM-Skript ist für die Standortregel konfiguriert.

   Hinweis: Wenn Sie das Skript angeben, lassen Sie die Spalten "Scalability-Server" und "Subnetz-Scanning" leer. Wenn Sie das Subnetz-Scanning nicht verwenden, lassen Sie die Spalte "Subnetz-Scanning" leer.

Beispiel:

```
rem ---------------------------------------------------------------------
rem Simple location aware server identification script
rem This script writes a hard coded server name to the output file
rem ---------------------------------------------------------------------

dim sMatchingAddress as string
```

```
dim sOutputFileName as string
dim sErrorFileName as string

dim X als Integer
FOR X=0 to argc()

        rem Read the output file from the provided parameters

        if ( argv(X)="-o") THEN
        sOutputFileName = argv(X+1)
        ENDIF

        rem read the matching address from the provided parameters

    if ( argv(X)="-a") THEN
        sMatchingAddress = argv(X+1)
        ENDIF

        rem read the matching address from the provided parameters

        if ( argv(X)="-x") THEN
        sErrorFileName = argv(X+1)
        ENDIF

NEXT X

dim fHandle as integer

fHandle = OpenFile(sOutputFileName,O_WRITE)
IF NOT(EOF(fHandle)) Then
        WriteFile(fHandle,"sampleserver.ca.com")
        CloseFile(fHandle)
        exit
ENDIF
exit
```

(Optional) Konfigurieren des Zeitlimits für Scan

Wenn Sie Subnetz-Scanning verwenden, bestimmt die Konfiguration "Zeitlimit für Scan" das maximale Intervall, in dem der Scan auf eine Antwort des Scalability-Servers wartet.

Gehen Sie wie folgt vor:

1. Doppelklicken Sie auf "Configure Scan Timeout" (Zeitlimit für Scan konfigurieren), und klicken Sie dann auf "Eigenschaften der Einstellung" im Portlet "Tasks".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

2. Ändern Sie das Feld "Wert" entsprechend für Ihre Umgebung, und klicken Sie dann auf "OK".

   Standard: 30

   Der Parameter "Configure Scan Timeout" (Zeitlimit für Scan konfigurieren) ist konfiguriert.

(Optional) Konfigurieren des Skript-Zeitlimits

Die Konfiguration "Skript-Zeitlimit" bestimmt das maximale Intervall, in dem das Skript ausgeführt werden soll. Die Skripte werden angehalten, wenn das angegebene Intervall abläuft.

Gehen Sie wie folgt vor:

1. Wählen Sie "Skript-Zeitlimit" aus, und klicken Sie dann im Portlet "Tasks" auf "Eigenschaften der Einstellung".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.

2. Ändern Sie das Feld "Wert" entsprechend für Ihre Umgebung, und klicken Sie dann auf "OK".

   Werte:

   - **0:** Ohne Zeitlimit
   - **>0:** Anzahl der Sekunden, die das Skript bis zum Zeitlimit ausgeführt werden soll
   - **Der höchste zulässige Wert bis zum Zeitlimit:** 600 Sekunden (10 Minuten)

   Standard: 300

   Die Parametereinstellungen des Skript-Zeitlimits sind konfiguriert.

(Optional) Konfigurieren des Scheduler für "Standorterkennung aktualisieren"

Der Richtliniengruppenordner "Standorterkennung aktualisieren" enthält einen Job, durch den CAF sich in regelmäßigen Intervallen beim Server registriert. Um einen Richtlinienparameterwert zu ändern, doppelklicken Sie auf eine Richtlinie, um das Dialogfeld "Eigenschaften der Einstellung" anzuzeigen.

CAF-Scheduler: Befehlszeile

Gibt den CAF-Befehl an, der diesen Job ausführt.

Standard: Standorterkennung

CAF-Scheduler: Auszuschließende Tage

Listet die Tage auf, die aus dem Ablaufplan ausgeschlossen werden sollen. Geben Sie eine beliebige Kombination der folgenden Werte an: monday, tuesday, wednesday, thursday, friday, saturday und sunday. Trennen Sie mehrere Werte durch Leerzeichen.

Standard: leer

CAF-Scheduler: Aktiviert

Gibt an, ob der Job "Registrierung aktualisieren" aktiviert werden soll.

Standard: True

CAF-Scheduler: Stunde

Gibt bei täglichen Zeitplänen die Stunde an, zu der der Job ausgeführt werden soll. Diese Richtlinie wird nicht bei stündlichen und minütlichen Zeitplänen verwendet.

Standard: 12

CAF-Scheduler: Auszuschließende Stunden

Listet die Stunden auf, die aus dem Ablaufplan ausgeschlossen werden sollen. Geben Sie die Zeiten im 24-Stunden-Format an. Trennen Sie mehrere Werte durch Leerzeichen.

Standard: leer

CAF-Scheduler: Minute

Gibt bei täglichen Zeitplänen die Minute nach der Stunde an, zu der der Job ausgeführt werden soll. Diese Richtlinie wird nicht bei minütlich ausgeführten Jobs verwendet.

Standard: 0

CAF-Scheduler: Zufällige Minuten

Gibt an, wie viele Minuten die Funktion zu einem "random_minute"-Job hinzufügt. Der Job wird zu der angegebenen Zeit plus eine zufällige Anzahl von Minuten bis zum angegebenen Wert ausgeführt. Die Richtlinie führt einen Job in "ungenauen" regulären Intervallen aus, um die Last auf verschiedene Server zu verteilen, indem die Uhrzeit, zu der Agenten eine Verbindung herstellen, teilweise zufällig ausgewählt wird.

Standard: 90

CAF-Scheduler: Zufällige Jetztzeit

Gibt die Zeit (in Sekunden) an, innerhalb der ein "random_now"-Job initiiert wird. Die Job in einer zufälligen Anzahl von Sekunden bis zum angegebenen Wert ausgeführt. Diese Richtlinie stellt sicher, dass Computer, die zusammen starten, ihre Jobs nicht gleichzeitig initiieren.

Standard: 0

CAF-Scheduler: Nummer wiederholen

Gibt das Intervall zwischen Wiederholungen des Jobs an. Dieser Wert hängt vom Jobtyp ab. Wenn der Typ beispielsweise "Tag" ist, steht der Wert für die Anzahl der Tage zwischen den Jobausführungen.

Standard: 1

CAF-Scheduler: Jobtyp

Gibt den Typ des geplanten Intervalls an. Gültige Werte sind "Tag" (day), "Stunde" (hour) und "Minute" (minute). Sie können außerdem die folgenden optionalen Bezeichner hinzufügen:

random

Führt den Job mit einer zufälligen Zeit aus, die der angegebenen Jobzeit hinzugefügt wird, und zwar bis zum Wert von "Zufällige Minuten".

random_hour

Wird zu einer zufälligen Stunde während des Tages ausgeführt.

random_minute

Wird zu einer zufälligen Minute während einer Stunde ausgeführt.

now

Startet den Job umgehend sowie nach der angegebenen Jobzeit.

Trennen Sie mehrere Werte durch Leerzeichen.

Beispiele:

Führen Sie den "amagent"-Job jeden Tag um 14:30 Uhr aus:

```
type=”day”, repeat=1, hour=14, minute=30, cmd=”start
amagent”
```

Führen Sie den "amagent"-Job aus, wenn CAF gestartet wird und an jedem Tag danach (außer an Wochenenden) zu einer zufälligen Uhrzeit nach zwischen 1:00 Uhr und 2:30 Uhr:

```
type=”day now random”, hour=1, minute=0, randomminutes=90,
excludedays=”Saturday Sunday”, cmd=”start amagent”
```

Anwenden der Standorterkennung auf Agenten

Nachdem Sie eine Richtlinie erstellt und versiegelt haben, wenden Sie sie auf ein Asset (ein Computer oder eine Gruppe) an.

Gehen Sie wie folgt vor: (für ein Asset)

1. Navigieren Sie unter dem Knoten "Systemsteuerung" in der Baumansicht zum Ordner "Konfigurationsrichtlinie".
2. Klicken Sie mit der rechten Maustaste auf die Richtlinie, die Sie anwenden möchten, und wählen Sie im Kontextmenü die Option "Kopieren" aus.
3. Navigieren Sie in der Baumansicht zum Asset, auf dem Sie die Richtlinie anwenden möchten. Klicken Sie mit der rechten Maustaste auf dieses Asset, und wählen Sie im Kontextmenü die Option "Einfügen" aus.

   Die Richtlinie wird auf das Asset angewendet.

Gehen Sie wie folgt vor: (für mehrere Assets oder Gruppen)

1. Wählen Sie die Assets bzw. Gruppen in der Baumansicht aus.
2. Klicken Sie mit der rechten Maustaste auf die markierten Ziele, und wählen Sie "Einfügen" im Kontextmenü.

   Es wird ein weiteres Kontextmenü angezeigt.
3. Klicken Sie auf "Konfigurationsrichtlinien".

   Das Dialogfeld zum Planen von Richtlinien wird geöffnet.
4. Planen Sie die zu aktivierende Richtlinie.

   Hinweis: Wenn Sie Richtlinien auf ein einzelnes Asset oder auf eine Gruppe anwenden, dann aktiviert die Funktion die Schaltfläche "Anpassen und Vorschau". Die Funktion deaktiviert die Schaltfläche, wenn Sie eine Richtlinie in mehreren Assets oder Gruppen einfügen.
5. Klicken Sie auf "OK", um die Richtlinie auf die Assets oder Gruppen anzuwenden.

Sie haben die Funktion zur Standorterkennung für die DSM-Agenten erfolgreich aktiviert und konfiguriert.

Inventarisierung und Verwaltung von Geräten

Die Asset Management-Funktionen in CA IT Client Manager (CA ITCM) bieten Administratoren einen einfachen, automatisierten Mechanismus für die Inventarisierung und Verwaltung von Geräten in einem Unternehmensnetzwerk mit Hilfe eines Prozesses der Erkennung und Agentenbereitstellung. Die Zurverfügungstellung eines installierten Agenten auf den erkannten Geräten ermöglicht eine laufende zentralisierte Verwaltung und Steuerung der Geräte.

Dieser Abschnitt bietet Informationen zu den folgenden Asset Management-Funktionen:

- Basisinventar-Komponente (siehe Seite 71)
- Unterstützung für nicht residentes Inventar (siehe Seite 72)

Weitere Informationen zu den Funktionen, Komponenten und Anforderungen von Asset Management finden Sie im *Administratorhandbuch zu Asset Management*, das in der CA IT Client Manager-Dokumentation enthalten ist.

Basisinventar-Komponente

Die Basisinventar-Komponente erkennt eine dynamische Teilmenge an Hardwareinformationen zum lokalen Computer und stellt diese Informationen anderen DSM-Komponenten zur Verfügung. Die Details der Inventarinformationen hängen von der Hardware-Umgebung und von der Plattform ab, auf der sie ausgeführt wird.

Die Basisinventarinformationen umfassen die folgenden Hardwareinformationen:

- System (z. B. Asset-Tag, Modell, Prozessoren oder Speicher)
- Betriebssystem (z. B. Sprache, Betriebssystem, Service Pack oder Version)
- Systemgeräte (z. B. Netzwerk- oder Video-Adapter)
- Netzwerk (z. B. Computer- und Domänenname, IP-Adresse/IPv6 oder TCP/IP)
- Dateisysteme (z. B. lokale Dateisysteme oder Partitionierung)
- Systemstatus (z. B. letzter Hardware-Scan)

Hinweis: Unabhängig von der Sprache, in der CA IT Client Manager ausgeführt wird, werden die Inventarinformationen immer auf Englisch angezeigt.

Unterstützung für nicht residentes Inventar

Die Unterstützungsfunktion für nicht residentes Inventar (NRI) von Asset Management ergänzt die Inventarisierungsfunktionalität, indem sie Enterprise-Administratoren ermöglicht, ihre Netzwerke zu inventarisieren, ohne dass dauerhafte Auswirkungen auf die inventarisierten Geräte entstehen. NRI bietet eine Elective-Lösung, wobei Endanwender angewiesen werden, eine Webseite zur Erfassung des Systeminventars zu verwenden, sowie eine verwaltete Lösung, wobei der Enterprise-Administrator eine Inventarerfassung startet, beispielsweise anhand von Anmeldeskripts.

Die NRI-Unterstützung verwendet Komponenten aus dem regulären DSM-Agenten in Verbindung mit Asset Collector und der Webkonsole.

Für die Verwendung von NRI müssen mindestens eine Webkonsole (und die dazugehörigen Web-Services) und ein Asset Collector für jeden Domänen-Manager installiert sein, auf dem nicht residentes Inventar erfasst und gespeichert werden soll. Im einfachsten Szenario kann jeder Domänen-Manager eine einzelne Webkonsole und einen Asset Collector zusammen beherbergen. Bei umfangreicheren und in höherem Maße skalierbaren Szenarios können mehrere Scalability-Server Webkonsolen und Asset Collectors zusammen beherbergen.

NRI wird im Rahmen der Asset Management-Funktionalität über das Setup-Programm von CA IT Client Manager installiert. Die Konfiguration von NRI erfolgt über eine einfache Konfigurationsdatei (Skriptdatei).

NRI unterstützt die Bestandsaufnahme auf Windows, Linux und UNIX-Zielcomputern. Außerdem werden die Verwaltungskomponenten von NRI nur auf Managern und Scalability-Servern unter Windows unterstützt.

Beschränkungen von NRI

Wenn Sie NRI unter einem normalen Benutzerkonto ausführen, das über weniger Berechtigungen verfügt als der "root"-Benutzer (unter UNIX und Linux) oder das Administratorenkonto (unter Windows), dann wird weniger Inventar vom NRI-Agent aufgezeichnet als von einem normalen CA ITCM-Agent.

Basierend auf den Berechtigungen, unter denen NRI ausgeführt wird, erfasst der NRI-Agent so viele Informationen wie möglich.

Hinweis: Weitere Informationen zu NRI, finden Sie im *Asset Management-Administrationshandbuch*.

Kapitel 2: Planen der Infrastrukturimplementierung

In diesem Kapitel werden wichtige Informationen zu den Anforderungen und der Skalierbarkeit von CA IT Client Manager dargestellt. Diese Informationen müssen gelesen und verstanden werden, bevor Sie DSM-Komponenten bereitstellen.

Dieses Kapitel enthält folgende Themen:

Unterstützung für IPv6 (siehe Seite 73)
FIPS 140-2-Support (siehe Seite 80)
Failover-Unterstützung und Hardwareersatz (siehe Seite 82)
Konfigurieren von CA HIPS für die Installation von CA ITCM (siehe Seite 86)
Hinweise zu Komponenten der Infrastruktur (siehe Seite 87)
Interne Abhängigkeiten (siehe Seite 99)
Abhängigkeiten mit anderen Produkten unter Windows. (siehe Seite 100)
Abhängigkeiten mit anderen Produkten unter Linux und UNIX (siehe Seite 104)

Unterstützung für IPv6

IPv6 (Internetprotokoll Version 6) ist der Nachfolger von IPv4 und damit die zweite Version des Internetprotokolls, das zur allgemeinen Verwendung zur Verfügung steht. IPv6 stellt vernetzten Geräten mehr Adressen bereit, d. h. dass beispielsweise jedes Mobiltelefon und jedes mobile elektronische Gerät eine eigene Adresse haben kann.

IPv6 basiert auf 128-Bit-Adressierung, d. h. es steht ein beträchtlicher Adressbereich zur Verfügung. Dieser große Adressbereich ermöglicht nahezu unbegrenzte Hierarchien und Adressenzuordnungen zu bestimmten Domänen. Außerdem wurden die automatische Konfiguration, die Sicherheit, die vereinfachte Weiterleitung sowie andere Dienste verbessert.

CA ITCM ist mit IPv6 kompatibel und funktioniert sowohl in einer reinen IPv4- oder IPv6-Umgebung als auch in einer gemischten IPv4-/IPv6-Umgebung.

Das IPv6 ermöglicht, dass Netzwerkadapter mehrere IPv6-Adressen und sowohl IPv4- als auch IPv6-Adressen haben. Es wird dringend empfohlen, voll qualifizierte Domänennamen (FQDN) zum Identifizieren von Managern, Scalability-Servern usw. zu verwenden.

Einschränkungen im Kontext der IPv6-Unterstützung

Im Kontext der IPv6-Unterstützung in CA IT Client Manager (CA ITCM) gelten die folgenden Einschränkungen:

- Wenn Sie im Konfigurationsspeicher den Parameter "protocolprecedence" auf den Wert "ipv6,ipv4" setzen und eine Oracle-MDB verwenden, werden Sie feststellen, dass das Produkt langsamer wird. Dies liegt daran, dass die Verbindung zur Oracle-Datenbank zunächst über IPv6-Adressen versucht wird, was fehlschlägt, und erst danach der Vorgang über eine IPv4-Adresse wiederholt wird. Um diese Leistungseinbußen zu vermeiden und dennoch vorrangig IPv6-Adressen in anderen Produktkomponenten zu verwenden, erstellen Sie in der Registrierung folgendes DWORD mit dem Wert 1:
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Unicenter ITRM\
  UseIPv4ForDB.
- Die BS-Installationsverwaltung (OS Installation Management, OSIM) ist nur in Netzwerken verfügbar, die IPv4 unterstützen. Dies liegt daran, dass OSIM PXE voraussetzt, das wiederum IPv4 voraussetzt.
- CA ITCM unterstützt beim Ansprechen von Infrastrukturkomponenten keine lokalen Link-Adressen, mit Ausnahme der folgenden zwei Fälle:
  - Beim Herstellen einer Verbindung von einem Remote Control-Viewer zu einem Remote Control-Host kann eine lokale Link-Adresse in den Remote Control-Viewer eingegeben werden.
  - Bei der Verwendung von Remote Control zum Durchsuchen des lokalen Netzwerks werden lokale Link-Adressen angezeigt und können ausgewählt werden.

  Hinweis: Lokale Link-Adressen werden im Rahmen der Erfassung und Anzeige des Inventars erfasst und angezeigt.
- Die NOS-Download-Methode für einen Software Delivery (SD)-Job wird über reines IPv6 unter den folgenden Bedingungen nicht unterstützt:
  - Der Agent verwendet Samba oder NFS, wobei die Plattform keine Rolle spielt
  - Der Agent ist eine ältere Windows-Plattform als Windows Vista und verwendet Microsoft NOS

Wenn es sich bei der Windows-Plattform jedoch um Windows Server 2003 handelt, können die folgenden Schritte ausgeführt werden, um den NOS-Download zu aktivieren:

1. Der folgende Registrierungsschlüssel muss auf den Agent-Computern auf 1 gesetzt werden:

   HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)

2. Die beiden folgenden Hotfix-Updates müssen auf alle Agent-Computer angewendet werden, für die die DSM Scalability-Server-Bibliotheksfreigabe gemountet werden soll:

   http://support.microsoft.com/kb/947369/de-de

   http://support.microsoft.com/kb/950092/de-de

3. Der Hostname des Scalability-Server-Computers muss in eine globale IPv6-Adresse aufgelöst werden.

4. Die Scalability-Server-Bibliotheksfreigabe (die sich im comstore des Scalability-Servers befindet) muss einen Hostnamen (keine IP-Adresse) verwenden. Führen Sie die folgenden Befehle aus, um zu prüfen, ob eine IP-Adresse verwendet wird:

   ```
   ccnfcmda -cmd GetParameterValue -ps itrm/usd/shared -pn exportarchive
   ccnfcmda -cmd GetParameterValue -ps itrm/usd/shared -pn msiadminpathunc
   ```

   Falls einer der Befehle einen Wert zurückgibt, der eine IP-Adresse enthält, ersetzen Sie die Adresse mit Hilfe der folgenden Befehle durch einen Hostnamen:

   ```
   ccnfcmda -cmd SetParameterValue -ps itrm/usd/shared -pn exportarchive
   -v durch_Hostenamen_zu_ersetzende_IP
   ```

   ```
   ccnfcmda -cmd SetParameterValue -ps itrm/usd/shared -pn msiadminpathunc
   -v durch_Hostenamen_zu_ersetzende_IP
   ```

   Wenn beispielsweise "GetParameterValue" für "msiadminpathunc" "\\2001:db9:1:2:f045:c89:5c2:bdf5\SDMSILIB" zurückgegeben hat, lautet der neue Wert "\\foobar.testarea.ca.com\SDMSILIB".

   Hinweis: Für ausführlichere Information über den Ccnfcmda-Befehl zur Agentenkonfiguration tippen Sie "<command> /?" in der Befehlszeile eingeben.

In der Praxis verwendet Software Delivery, wenn die vorausgehend beschriebene NOS-Download-Methode fehlschlägt, wieder die Download-Methode ohne NOS. Wenn dies jedoch durch eine Änderung der Standardrichtlinie verhindert wird, schlägt der SD-Job unter diesen Umständen fehl.

- Die Mitgliedschaft in dynamischen Containern von Data Transport Service (DTS) WorldView unterstützt nur IPv4-Adressbereiche.

- Infrastructure Deployment und Continuous Discovery unterstützen nur IPv4-Adressbereiche.
- Der Assistent für nicht verwaltete Computer, mit dem der Benutzer ein oder mehrere Subnetze angeben kann, die zum Herausfiltern von nicht verwalteten Computern verwendet werden, unterstützt nur IPv4-Subnetze.
- Der CAF-Dienst-Locator funktioniert möglicherweise nur in einem lokalen Subnetz, was sich auf den Packager auswirken kann, der Manager dann nur im lokalen Subnetz findet. (Dies hängt davon ab, ob die Router den "Scoped Multicast" zulassen.)
- Das DTS PPP-Protokoll unterstützt IPv6 nicht.
- CA ITCM unterstützt nicht das Deaktivieren von IPv4 unter Windows Server 2003 und Windows XP, da das Deaktivieren von IPv4 auf diesen Windows-Plattformen generisch nicht unterstützt wird.
- Unter Windows Vista und Windows Server 2008 unterstützt CA ITCM reines IPv6. IPv4 muss auf diesen Plattformen entfernt werden, indem der folgende Befehl über eine Eingabeaufforderung ausgeführt wird:
  `netsh interface ipv4 uninstall`

  Wenn ein Neustart erforderlich ist, wird eine entsprechende Meldung angezeigt.

Konfigurationshinweise im Kontext der IPv6-Unterstützung

Im Kontext der IPv6-Unterstützung in CA IT Client Manager (CA ITCM) müssen Sie die folgenden Hinweise und Aspekte zur Konfiguration beachten.

- Konfigurationsparameter (Richtlinieneinträge) im DSM-Explorer steuern wie nachfolgend beschrieben die IPv6- und IPv4-Verbindungen:

  Rangfolge für DNS-Abfragen definieren

  Definiert die Rangfolge von DNS-Abfragen, wenn diese direkt, d. h. nicht mit Hilfe von allgemeinen Funktionen, ausgeführt werden. In älteren Betriebsumgebungen als Windows Vista wird DNS nur über IPv4 unterstützt.

  Standard: ipv4,ipv6

Rangfolge für Namensauflösungen definieren

Definiert die Rangfolge von Namensauflösungsfunktionen. In manchen Umgebungen ist die WINS- und NETBIOS-Namensauflösung möglicherweise zuverlässiger als DNS. In diesen Fällen können Sie festlegen, dass die NETBIOS-Auflösung vorrangig vor DNS-Abfragen verwendet werden soll.

Wenn dieser Parameter festgelegt ist, wird der Wert des Konfigurationsparameters "Fallback mit NETBIOS-Kurznamen verwenden" ignoriert, und die Namensauflösung fragt zuerst NETBIOS ab, indem sie den FQDN auf einen Kurznamen reduziert, bevor sie wieder auf DNS und andere Methoden zurückgreift. Wenn bereits eine infolge dieser Richtlinie veranlasste Kurznamensabfrage ausgeführt wurde, wird, sofern aktiviert, der Kurznamens-Fallback übersprungen. Dieser Parameter wird nur auf CA ITCM-Systemen unterstützt, die NETBIOS-Abfragen unterstützen.

Hinweis: Dieser Parameter wird zurzeit nicht verwendet.

Standard: dns,netbios

Rangfolge für aufgelöste Adressen definieren

Definiert die Rangfolge der IP-Adressfamilie (IPv6 oder IPv4), wenn mehrere IP-Adressfamilien verwendet werden.

Wenn Adressen aufgelöst werden, gibt dieser zentral verwaltete Parameter an, welche Priorität den einzelnen Adressfamilien zugewiesen werden soll. Standardmäßig werden zuerst IPv4-Adressen und dann IPv6-Adressen angefordert, um die maximale Interoperabilität aufrechtzuerhalten.

Standard: ipv4,ipv6

IPv4-Auflösung aktivieren

Aktiviert die Unterstützung für die IPv4-Adressauflösung. Dieser Parameter ist nur ein Platzhalter in der aktuellen Version der Software. Daher ignorieren Endknoten diese Einstellung und unterstützen die IPv4-Auflösung immer.

Standard: True

IPv6-Auflösung aktivieren

Aktiviert die Unterstützung für die IPv6-Adressauflösung, so dass IPv6-Adressen zurückgegeben werden können. Wenn dieser Parameter deaktiviert (Falsch) ist, entfernt der Resolver alle IPv6-Adressen aus den Ergebnissen der Namensauflösung.

Hinweis: Dieser Parameter wird im Gegensatz zum entsprechenden IPv4-Parameter von den Endknoten berücksichtigt.

Standard: True

Datenbank als Fallback für die Namensauflösung verwenden

Gibt einen Fallback auf eine IP-Adresse an, die auf der MDB-Datenbank eines Managers oder auf einer Datenbank eines Servers gespeichert ist, wenn ein Live-Name nicht durch Adressermittlungsdienste (DNS) oder NETBIOS aufgelöst werden kann.

Hinweis: Die Standard-Fallback-Option sollte in den meisten Fällen beibehalten und nur dann geändert werden, wenn dies von Mitarbeitern des Technischen Supports von CA verlangt wird.

Folgende Werte sind gültig:

1 = Alle Fallback-Modi aktiviert

2 = Server-Datenbank-Fallback verwenden

4 =MDB-Fallback verwenden

Standard: 1

Fallback mit NETBIOS-Kurznamen verwenden

Gibt an, ob NETBIOS-Kurznamen als Fallback verwendet werden, wenn die FQN-Abfrage fehlschlägt.

Standard: True

Hinweis: Diese Konfigurationsparameter befinden sich im Fensterbereich "Konfigurationsrichtlinie/Standardcomputerrichtlinie/DSM/Allgemeine Komponenten/Netzwerk/Allgemein". Ausführlichere Informationen finden Sie unter dem Thema "Richtliniengruppe 'Allgemein' (Netzwerk)" im Abschnitt "Konfigurationsrichtlinie" der *DSM-Explorer-Hilfe*.

- Wenn CA ITCM auf einem Computer installiert wird, auf dem nur IPv4 aktiviert ist, und dann zu einem späteren Zeitpunkt IPv6 aktiviert wird, müssen der Computer und der CAF-Dienst neu gestartet werden.
- Wenn Ihr Netzwerk nur IPv6 unterstützt (also die IPv4-Weiterleitung deaktiviert oder gestoppt wurde) oder hauptsächlich IPv6-Verbindungen verwendet, wird empfohlen, dass Sie den Wert des Konfigurationsparameters "Rangfolge für aufgelöste Adressen definieren" in "ipv6,ipv4" ändern. Diese Einstellung verbessert die Kommunikationsleistung zwischen den verschiedenen Computern im Enterprise oder in der Domäne.
- Wenn Sie einen Manager mit einer Remote-MDB und ausschließlich die IPv6-Weiterleitung zwischen dem Manager und der Remote-MDB verwenden, wird der DSM-Explorer beim ersten Mal sehr langsam geöffnet, da der Konfigurationsparameter "Rangfolge für aufgelöste Adressen definieren" anfänglich standardmäßig auf "ipv4,ipv6" gesetzt ist. In diesem Fall wird der Name zuerst in eine IPv4-Adresse aufgelöst, die Datenbankverbindung schlägt nach einer Zeitüberschreitung fehl, anschließend wird der Vorgang mit der IPv6-Adresse versucht, und dies hat Erfolg. Die Konfigurationsrichtlinie kann nur nach dem Öffnen des DSM-Explorers geändert werden.

- Wenn sich in ihrem Netzwerk eine größere Anzahl von Windows 2003- und Windows XP-Computern befindet, lassen Sie den Konfigurationsparameter "Rangfolge für DNS-Abfragen definieren" auf "ipv4,ipv6" gesetzt, da auf diesen Plattformen DNS-Meldungen nur über IPv4-Verbindungen gesendet werden.

DNS-Namensauflösung für DSM-Komponenten hostende Computer

Alle DSM-Komponenten (beispielsweise Enterprise-Manager, Domänen-Manager, Scalability-Server und Agents) hostenden Computer müssen vorwärts- und rückwärtsgerichtete DNS-Abfragen unterstützen. Überprüfen Sie, ob die Kommunikation zwischen den DSM-Komponenten richtig funktioniert.

Zuweisen eines Hostnamens für den Loopback einer IP-Adresse

CA ITCM erfordert, dass der Hostname für interne und externe Kommunikationen zu jeder Zeit auflösbar ist. Das interaktive Installationsprogramm enthält die Option "Assigned hostname to the loopback IP" (Der Loopback-IP-Adresse zugewiesener Hostname), womit die vorherige Option festgelegt werden kann.

Legen Sie den Eintrag "write_hostname" bei einer unbeaufsichtigten Installation im Netzwerk- oder DNS-Bereich wie folgt auf "Wahr" fest:

```
<networking>
  <dns>
    <dhcp_hostname config:type="boolean" >false</dhcp_hostname>
    <dhcp_resolv config:type="boolean" >true</dhcp_resolv>
    <hostname>$HostName$</hostname>
    <write_hostname config:type=boolean>true</write_hostname>
  </dns>
</networking>
```

Die Datei "autoinst.xml" befindet sich unter folgendem Speicherort:

DSM_Install_Folder\server\SDBS\var\managedpc\images\IMAGE_NAME\IMAGE_NAME\suse

FIPS 140-2-Support

Der Federal Information Processing Standard (FIPS) Veröffentlichung 140-2 (FIPS PUB 140-2) ist ein Computer-Sicherheitsstandard der US-Regierung für die Zertifizierung kryptographischer Module. Dieser Standard wird vom National Institute Of Standards And Technology (NIST) veröffentlicht und aktualisiert.

Computer-Produkte, die FIPS 140-2-zertifizierte kryptographische Module in ihrem FIPS-zertifizierten Modus verwenden, dürfen nur von FIPS anerkannte Sicherungsfunktionen wie AES (Advanced Encryption Standard), SHA-1 (Secure Hash Algorithm), und Protokolle höherer Ebenen wie TLS v1.0 verwenden, die ausdrücklich in den FIPS 140-2-Standards und -Implementierungshandbüchern erlaubt sind.

Kryptographie in CA ITCM befasst sich mit den folgenden Aspekten:

- Speicherung und Prüfung von Kennwörtern
- Kommunikation aller vertraulichen Daten zwischen Komponenten von CA-Produkten und zwischen CA-Produkten und Drittparteien-Produkten

FIPS 140-2 legt die Anforderungen für die Verwendung kryptographischer Algorithmen innerhalb eines Sicherheitssystems fest, das vertrauliche aber nicht geheime Daten schützt.

CA ITCM unterstützt FIPS-konforme Verfahren für Kryptographie. CA ITCM umfasst die kryptographischen Bibliotheken RSA BSafe und Crypto-C ME v2.1, die als den Anforderungen von FIPS 140-2 für kryptographische Bibliotheken entsprechend validiert worden sind.

FIPS 140-2-Plattform-Support

Um Konformität mit FIPS 140-2 zu erreichen, muss ein FIPS 140-2-zertifiziertes Kryptographiemodul verwendet werden. Das zertifizierte RSA-Kryptographiemodul steht für Plattformen, die über CA ITCM verfügen, nicht zur Verfügung. Für Plattformen, für die kein zertifiziertes Modul verfügbar ist, in deren Domänenrichtlinie jedoch nur FIPS 140-2-Kryptographie festgelegt ist, verwendet die kryptographische Unterstützung Algorithmen und Funktionen, die FIPS-genehmigt sind, jedoch von einem nicht genehmigten kryptographischen Modul (CA OpenSSL) zur Verfügung gestellt werden.

Folgende Plattformen sind FIPS 140-2-konform, wenn sie im Nur-FIPS-Modus betrieben werden:

- Windows NT x86-Plattformen
- Linux
- Solaris SPARC/32

Sämtliche andere Plattformen sind derzeit nicht 140-2-konform. Wenn Sie für Nur-FIPS-Modi konfiguriert sind, verwenden sie ausschließlich von FIPS genehmigte Algorithmen und Funktionen. Sie verwenden jedoch keinen zertifizierten kryptographischen Provider.

Unterstützte FIPS-Modi

CA ITCM unterstützt FIPS-konforme Kryptographie in zwei Modi - "FIPS-bevorzugt" und "nur-FIPS". Die beiden Modi können für die Speicherung und Prüfung von Kennwörtern und die Kommunikation aller vertraulichen Daten zwischen Komponenten von CA-Produkten und zwischen CA-Produkten und Drittanbieter-Produkten verwendet werden.

Modus "FIPS-bevorzugt"

Bezieht sich auf den Modus, der Rückwärtskompatibilität mit früheren Versionen von CA ITCM bietet. In diesem Modus verwenden die Version 12.8-Komponenten FIPS-kompatible Kryptographie, während sie mit einer anderen Version 12.8-Komponente kommuniziert. Wenn sie mit den Komponenten früherer Versionen kommunizieren, können sie allerdings Sicherungsfunktionen verwenden, die nicht FIPS-konform sind, um Rückwärtskompatibilität zu unterstützen. Während "FIPS-bevorzugt" der Standardmodus für Neuinstallationen ist, ist er der *einzige* unterstützte Modus für Upgrades.

Hinweis: Nachdem Sie das Upgrade aller DSM-Komponenten in Ihrer Umgebung durchgeführt haben, können Sie auf "Nur-FIPS"-Modus umschalten.

"Nur-FIPS"-Modus

Bezieht sich auf den Modus, der nur FIPS-konforme Verfahren für Kryptographie verwendet. Verwenden Sie diese Option für *neue* CA ITCM-Installationen. Dieser Modus ist nicht rückwärtskompatibel mit früheren Versionen von CA ITCM.

Hinweis: Nachdem Sie in den "Nur-FIPS"-Modus gewechselt haben, können die Komponenten frühere Kryptographie nicht verwenden. Sie können bei Bedarf auf den Modus "FIPS-bevorzugt" zurückgreifen.

Weitere Informationen:

So wechseln Sie in "nur-FIPS" (siehe Seite 454)
So wechseln Sie in "FIPS-bevorzugt" (siehe Seite 455)

Failover-Unterstützung und Hardwareersatz

CA IT Client Manager unterstützt Failover in einer Cluster-Umgebung sowie das Ersetzen der Managerhardware im Falle eines Hardwareausfalls oder einer Hardwareaktualisierung.

Weitere Informationen finden Sie in folgenden Abschnitten:

- Failover-Unterstützung (siehe Seite 82)
- Ersetzen von Managerhardware (siehe Seite 85)

Failover-Unterstützung

Die Failover-Unterstützung ist nur für Windows-Betriebsumgebungen und Microsoft-SQL Server-Datenbanken verfügbar.

Failover unterstützt die Installation der Managerkomponenten auf zwei verschiedenen Computern, auf denen Microsoft Cluster ausgeführt wird. Ein System muss der aktive Knoten sein, der die Managerfunktionalität ausführt. Bei dem anderen System (ggf. auch mehrere) handelt es sich um ein passives Standby-System, auf dem die Managersoftware installiert, aber nicht aktiviert ist.

Installation auf einem Cluster

CA ITCM verfügt über keine Funktion, mit der Systemfehler erkannt werden und im Falle eines Systemfehlers vom aktiven auf den passiven Knoten gewechselt werden kann.

CA ITCM kann auf zwei Arten installiert werden: als aktiver ITCM-Manager oder als passiver ITCM-Manager. Die Begriffe "Aktiv" und "Passiv" beziehen sich darauf, ob der DSM-Manager aktiv oder passiv ist. Sie beziehen sich nicht auf den Knoten "Cluster" (der ebenfalls aktiv oder passiv sein kann).

Wenn CA ITCM in einem Cluster installiert wird, wird eine Instanz des DSM-Managers als aktiver ITCM-Manager und die anderen Instanzen als passive ITCM-Manager installiert.

So installieren Sie einen aktiven ITCM-Manager:

1. Starten Sie im aktiven Knoten des Clusters das CA ITCM-Installationsprogramm auf die übliche Weise, und führen Sie eine benutzerdefinierte Installation aus.
2. Wählen Sie die Managerkomponenten und CCS sowie alle anderen zu installierenden Komponenten.

   CCS ist bei der Installation in einer Cluster-Umgebung eine obligatorische Komponente. CCS installiert die Hochverfügbarkeitsdienst-Option, die für die Cluster-Unterstützung benötigt wird.

3. Geben Sie im Dialogfeld "Manager konfigurieren" den Namen des Management-Datenbankservers ein.
4. Klicken Sie auf die Schaltfläche "Wiederherstellung".
5. Wählen Sie im angezeigten Dialogfeld die Optionen "Wiederherstellungsunterstützung aktivieren" und "Aktiv".
6. Geben Sie den Namen des Clusters und den Speicherort des freigegebenen Laufwerks ein.

   Hinweis: Wenn Sie einen DSM-Domänen-Manager mit einem lokalen Microsoft SQL Server in einer Microsoft-Cluster-Umgebung installieren möchten, muss CA ITCM in der Microsoft SQL Server-Clustergruppe, unter Verwendung des virtuellen Namen des Microsoft SQL Servers, installiert werden.
7. Fahren Sie mit der Installation fort bis zum Dialogfeld "Zielspeicherort auswählen", in dem Sie den Zielordner konfigurieren.

   Der Zielordner muss sich auf der Festplatte des Computers (nicht auf der freigegebenen Festplatte des Clusters) befinden.

   Der Speicherort der Konfigurationsdaten muss auf die freigegebene Festplatte des Clusters verweisen. Dies erfolgt automatisch basierend auf den im Dialogfeld "Failover" eingegebenen Informationen. Sie können jedoch diese Speicherorte überprüfen, indem Sie auf die Schaltfläche "Erweitert" klicken. Der Speicherort der freigegebenen Komponenten muss sich ebenfalls auf der lokalen Festplatte des Computers befinden. Dieser Speicherort wird auch mit Hilfe der Schaltfläche "Erweitert" konfiguriert.
8. Klicken Sie auf "Weiter", und durchlaufen Sie die Dialogfelder des Installationsprogramms, bis die Installation gestartet wird.

   Die Installation eines Managers auf einem Cluster-Computer unterscheidet sich geringfügig von einem eigenständigen, nicht geclusterten Computer. Die Installation von CCS verläuft in der Regel im Hintergrund. Auf einem Cluster ruft CA ITCM jedoch eine interaktive Installation von CCS auf.

   Wichtig! Ändern Sie keine Informationen in diesen Dialogfeldern, da CA ITCM ihnen bereits die entsprechenden Werte zugewiesen hat. Durchlaufen Sie die Dialogfelder so lange mit "Weiter", bis die CCS-Installation startet.

So installieren Sie einen passiven ITCM-Manager:

1. Bevor Sie die Installation auf einem anderen Computer (oder anderen Computern) des Clusters durchführen, müssen Sie sicherstellen, die Clustergruppen verfügbar und die freigegebenen Ressourcen funktionsfähig sind. Alternativ können Sie den Computer zum aktiven Knoten im Cluster machen.
2. Starten Sie das CA ITCM-Installationsprogramm wie üblich, und führen Sie eine benutzerdefinierte Installation aus.

3. Wählen Sie dieselben Komponenten aus wie bei der Installation des aktiven ITCM-Managers.
4. Geben Sie im Dialogfeld "Manager konfigurieren" den Namen des Management-Datenbankservers ein.
5. Klicken Sie auf die Schaltfläche "Wiederherstellung".
6. Wählen Sie im angezeigten Dialogfeld die Optionen "Wiederherstellungsunterstützung aktivieren" und "Passiv".
7. Als Nächstes fragt das Installationsprogramm nach dem Speicherort der DSMRecovery.ini-Datei.

   Diese Datei befindet sich auf der freigegebenen Festplatte des Clusters im Verzeichnis mit den CA ITCM-Konfigurationsdaten. Der tatsächliche Speicherort wird während der Installation des aktiven ITCM-Managers definiert.
8. Klicken Sie auf "Weiter", und durchlaufen Sie die Dialogfelder des Installationsprogramms, um die Installation zu starten.

   Wie auch die Installation des aktiven ITCM-Managers verläuft die CCS-Installation interaktiv.

   Wichtig! Ändern Sie auch hier keine Informationen in den Dialogfeldern, da CA ITCM ihnen bereits die entsprechenden Werte zugewiesen hat. Durchlaufen Sie die Dialogfelder so lange mit "Weiter", bis die CCS-Installation startet.

Wenn die Installationen abgeschlossen sind, können die Cluster-Ressourcen zurück auf den aktiven Knoten des Clusters verschoben werden.

Wenn der aktive Knoten des Clusters zwischen den Computern im Cluster wechselt, muss der passive ITCM-Manager hiervon benachrichtigt werden. Diese Benachrichtigung erfolgt durch Ausführen der Datei "ActivateManagerNode.bat", die sich im Verzeichnis "bin" am Installationsspeicherort des DSM-Managers befindet. Alternativ kann der Cluster-Manager in einem Cluster-Management-System so konfiguriert werden, dass er den Inhalt der Datei "ActivateManagerNode.bat" ausführt.

Hinweise:

- Weitere Informationen zur Einrichtung von Clusters finden Sie im grünen Papier mit dem Titel "CA ITCM/CAUnicenter Desktop & Server Management" unter http://ca.com/greenbooks
- Wenn Sie in einer nicht standardmäßig benannten SQL-Instanz installieren, stellen Sie sicher, dass die TCP/IP-Port-Nummern der Instanz auf allen Knoten im Cluster identisch sind. Falls nicht, müssen Sie die Port-Nummern entsprechend anpassen. Stellen Sie auch sicher, dass der SQL-Server-Browser ausgeführt wird.
- Derzeit wird ein Boot-Server auf einem Cluster nicht unterstützt.

- Unter Windows 2008 (und Windows Vista) muss die Befehlsdatei "ActivateManagerNode.bat" mit vollen Administratorrechten ausgeführt werden. Wenn Sie als Administrator angemeldet sind, verfugen Sie automatisch über volle Rechte. Wenn Sie jedoch als ein anderer Benutzer aus der Administratorgruppe angemeldet sind, weist Ihnen Windows nur normale Benutzerrechte zu, sodass Sie die Befehlsdatei nicht erfolgreich ausführen können. Um dies zu ändern, muss die Befehlsdatei "ActivateManagerNode.bat" als Benutzer mit erhöhten Berechtigungen ausgeführt werden. Um z. B. ein Befehlszeilenfenster mit erhöhten Berechtigungen zu öffnen, klicken Sie mit der rechten Maustaste auf das Eingabeaufforderungssymbol und wählen Sie "Als Administrator ausführen". Anschließend kann die Befehlsdatei von hier aus ausgeführt werden.

Ersetzen von Managerhardware

Im Falle eines Systemausfalls oder einer Hardwareaktualisierung kann die Hardware des Managersystems so ersetzt werden, dass die Original-MDB und die Konfigurationseinstellungen weiter verwendet werden können.

Es ist nicht erforderlich, die MDB erneut zu installieren oder die Software Delivery-Bibliothek oder die Remote Control-Adressbücher neu zu konfigurieren, da die ursprüngliche Konfiguration beibehalten werden kann.

Um sich auf Fälle vorzubereiten, in denen das Managersystem ersetzt werden muss, müssen Sie einige Einstellungen im Installationsassistenten vornehmen. Im Dialogfeld "Manager konfigurieren" gelangen Sie über die Schaltfläche "Wiederherstellen" zum Dialogfeld für Failover. In diesem Dialogfeld müssen Sie die Optionen "Systemersetzung" und "Ersetzung aktivieren" auswählen. Legen Sie im Dialogfeld für die Installationsverzeichnisse die Verzeichnisse für Managerdaten (MDB- und Konfigurationsdaten) auf einen Pfad fest, der regelmäßig gesichert werden muss. Während der Installation werden alle Eingaben in den Dialogfeldern in der Datei "DSMRecovery.ini" gespeichert, die sich am angegebenen Speicherort für Konfigurationsdaten befindet. Mit dieser Datei können Sie die Hardware nach einem Absturz ersetzen.

Wenn die Hardware ersetzt wurde und der Manager neu installiert werden muss, rufen Sie das Dialogfeld "Wiederherstellen" erneut auf und wählen die Optionen "Ersetzung aktivieren" und "System wird ersetzt" aus.

Unten muss der Installationspfad für die Konfigurationsdaten eingegeben werden, damit der Installer die ursprünglich gespeicherte Datei "DSMRecovery.ini" finden kann. Der Installer liest alle Installationsparameter und verwendet dieselbe MDB, Softwarebibliothek usw. wie bei der ursprünglichen Managerinstallation.

Der relative Pfad zu den Konfigurationsdaten muss mit dem Pfad übereinstimmen, der für den aktiven Manager galt.

Beim Ersetzen des Managersystems muss die alte und die neue Managerhardware denselben Systemnamen verwenden.

Hinweis: Im Falle eines Ausfalls der Computerhardware kann die Datenkonsistenz nicht gewährleistet werden.

Konfigurieren von CA HIPS für die Installation von CA ITCM

Wenn Sie CA ITCM auf einem Computer installieren, auf dem ein CA HIPS-Client (CA Host-Based Intrusion Prevention System) installiert ist, müssen Sie den CA HIPS-Server konfigurieren, bevor Sie CA ITCM auf dem Client-Computer installieren können.

So konfigurieren Sie CA HIPS für die Installation von CA ITCM:

1. Melden Sie sich auf dem CA HIPS-Servercomputer bei der CA HIPS-Konsole an.
2. Klicken Sie auf "Richtlinien-Management", "Definitionen", "Anwendungs-Repository".
3. Wenn die Gruppenliste keine SafeApps-Gruppe enthält, erstellen Sie eine Gruppe mit dem Namen "SafeApps" und führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf "Richtlinien-Management", "Definitionen", "Allgemeine Einstellungen", "Globale Einstellungen für Betriebssystemsicherheit".
   b. Wählen Sie in der Dropdown-Liste "Anwendungsgruppe zum Umgehen von Benutzermodus-Hooks" die Option "SafeApps", und klicken Sie auf "OK".
   c. Klicken Sie auf "Richtlinien-Management", "Definitionen", "Anwendungs-Repository".
4. Wählen Sie die Gruppe "SafeApps" aus.
5. Klicken Sie auf "Neue hinzufügen", und geben Sie die folgenden Details ein, um die Datei "setup.exe" zu definieren:

Feld	Wert
Elementtyp	Anwendung
Mitgliedsname	setup.exe
Identifizieren durch	FileName
Pfad	setup.exe
Gruppen	SafeApps

6. Klicken Sie auf "OK".

7. Klicken Sie auf "Neue hinzufügen" und geben Sie die folgenden Details ein, um die Datei "CACMS.MSI" zu definieren:

Feld	Wert
Elementtyp	Anwendung
Mitgliedsname	CACMS.MSI
Identifizieren durch	FileName
Pfad	CACMS.MSI
Gruppen	SafeApps

8. Klicken Sie auf "OK".
9. Klicken Sie auf "Richtlinien-Management", "Bereitstellung".
10. Klicken Sie auf "Bereitstellen".
11. Geben Sie eine Versionsnummer an, und klicken Sie auf "OK".
12. Warten Sie die Aktivierung der Richtlinie auf dem CA HIPS-Clientcomputer ab.

    Der CA HIPS-Clientcomputer ist jetzt bereit für die Installation von CA ITCM.

Hinweise zu Komponenten der Infrastruktur

Die Beziehung zwischen den unterschiedlichen Komponenten von CA ITCM gestaltet sich folgendermaßen:

- Zwischen Agenten und ihrem Scalability-Server besteht eine 1:n-Beziehung. Jeder Agent muss Meldungen an einen einzigen Scalability-Server senden.
- Scalability-Server können eine 1:n-Beziehung zu ihrem Domänen-Manager haben. Jeder Scalability-Server muss Meldungen an einen einzigen Domänen-Manager senden.
- Domänen-Manager haben eine optionale 1:n-Beziehung zu einem Enterprise-Manager. Jeder Domänen-Manager kann nur einem Enterprise-Manager unterstehen.

Schritte zur Installation der Infrastruktur

Eine erfolgreiche Installation der Infrastruktur erzielen Sie durch folgende Vorgehensweise:

- Festlegen der richtigen Position der Komponente.

  In diesem Schritt wird festgelegt, welche Computer welche Rolle übernehmen. Dabei sind u. A. Aspekte wie Netzwerkbandbreite und vorhandene Systemauslastung zu berücksichtigen.

- Prüfen, ob das Netzwerk ordnungsgemäß konfiguriert ist

  Die DNS-Konfiguration muss eine erfolgreiche Ausführung des Befehls "nslookup *IP-Adresse*" für vertikale Verbindungen entlang der CA ITCM-Ebenenhierarchie (Enterprise-Manager – Domänen-Manager, Domänen-Manager – Scalability-Server, Scalability-Server – Agent, Domänen-Manager – Agent) ermöglichen.

- Installieren der Enterprise- und Domänen-Manager.
- Installieren der Scalability-Server.
- Installieren der Agenten.
- Installieren der Verwaltungskonsolen des DSM-Explorers

Schlüsselfaktoren bei der Größenfestlegung der Infrastruktur

Eine Reihe von Schlüsselfaktoren haben beträchtlichen Einfluss auf die Größe der Infrastruktur und die Systemleistung.

Auslastung für Asset Management-Tasks

Die Größe der Infrastruktur hängt von der Auslastung der folgenden Asset Management-Tasks ab:

- Anzahl der erfassten Inventarattribute
- Häufigkeit der Inventarerfassung

Auslastung für Software Delivery-Tasks

Die Größe der Infrastruktur hängt von der Auslastung der folgenden Software Delivery-Tasks ab:

- Größe der zu liefernden Softwarepakete
- Menge der zu liefernden Softwarepakete
- Management der Netzwerkbandbreite
- Häufigkeit der Lieferung von Softwarepaketen (täglich, wöchentlich, monatlich usw.)

Computeridentifikation in CA ITCM

CA ITCM weist jedem verwalteten Computer eine CA Technologies-spezifische UUID zu (Universal Unique Identifier, universelle eindeutige ID). Diese wird auf jedem Computer am folgenden Speicherort abgelegt:

Windows-Registrierung:

`HKEY_LOCAL_MACHINE\Software\ComputerAssociates\HostUUID`

Linux/UNIX:

`/etc/cadmuuid`

Das CA ITCM Anwendungs-Framework (CAF) überprüft die Speicherorte in regelmäßigen Abständen nach einer CA Technologies-spezifischen UUID. Wenn eine UUID gefunden wird, geht CAF davon aus, dass dieses Asset bereits in der Datenbank registriert wurde. Wenn keine CA Technologies-spezifische UUID gefunden wird, erstellt CAF eine neue CA Technologies-spezifische UUID und registriert das Asset in der Datenbank.

Wenn Sie eine Installation kopiert haben (eine physische Speicherung der Festplatte, die mit einem Imaging-Tools wie z. B. GHOST erstellt wurde, oder eine Image-Datei eines virtuellen Computers, die mit einem Tool wie z. B. VMware erstellt wurde), um sie auf einem anderen Computer zu installieren oder als Sicherungskopie zu verwenden, so enthält diese kopierte Installation eine CA-spezifische UUID des ursprünglichen Computers. Wenn Sie diese kopierte Installation nicht auf dem ursprünglichen Computer starten, wird die CA-spezifische UUID zwei Mal angezeigt.

Um eine Duplizierung der CA-spezifischen UUID zu vermeiden, führt CA ITCM die folgenden Aktionen aus:

1. Wenn CAF gestartet oder der Befehl “caf register” ausgeführt wird, wird durch einen Algorithmus geprüft, ob der Zielcomputer mit dem ursprünglichen Computer übereinstimmt.
2. Wenn der Zielcomputer mit dem ursprünglichen Computer übereinstimmt, wird die ursprüngliche CA-spezifische UUID verwendet. Anderenfalls wird eine neue CA-spezifische UUID erstellt.

Um die Notwendigkeit einer eindeutigen CA-spezifischen UUID festzustellen, kann CA ITCM entweder den Standard-Algorithmus (empfohlen) oder den Legacy-Algorithmus verwenden. Der Algorithmus vergleicht folgende Eigenschaften des Zielcomputers mit den Werten in der Datenbank:

Virtueller Computer

Die System-ID (ein System-BIOS-Attribut) ist die einzige Eigenschaft, die durch den Algorithmus überprüft wird.

Physicher Computer

- Übereinstimmung der MAC-Adresse

  Wenn mindestens eine der MAC-Adressen des Ziels mit einer der ursprünglichen MAC-Adressen übereinstimmt, ist dieses Kriterium erfüllt.

- Übereinstimmung der Seriennummern der Festplatten

  Wenn mindestens eine der Seriennummern der Festplatten auf dem Ziel mit einer der ursprünglichen Seriennummer der Festplatten übereinstimmt, ist dieses Kriterium erfüllt.

- Übereinstimmung der System-ID

  Wenn die System-ID mit der ursprünglichen System-ID übereinstimmt, ist dieses Kriterium erfüllt.

Änderungen der Werte der genannten Eigenschaften machen nicht in jedem Fall Änderungen der CA-spezifischen UUID erforderlich. Unter den folgenden Umständen initiiert der Algorithmus eine Änderung der CA-spezifischen UUID:

- Der Wert wird nur dann geändert, wenn der ursprüngliche Wert der Eigenschaft in der Datenbank vorhanden ist und sich der neue Wert von ihm unterscheidet.

  Wenn z. B. die alte Liste der MAC-Adressen für den Vergleich nicht in der Datenbank verfügbar ist, wird *keine Änderung* der CA-spezifischen UUID ausgelöst.

- Der Wert wird nur dann geändert, wenn die neuen Werte der MAC-Adressen oder der Seriennummern der Datenträger mit den in der Datenbank bestehenden Werten übereinstimmen.

Sperren der Host-UUID

Eine Hardwareänderung zieht normalerweise eine Änderung der Host-UUID nach sich. Wenn Sie dies verhindern möchten, können Sie die Host-UUID sperren.

- Um die Host-UUID unter Windows zu sperren, müssen Sie unter dem Registrierungsschlüssel "HKLM\Software\ComputerAssociates\HostUUID" einen Zeichenfolgewert "LockHostUUID" mit dem Wert “1” erstellen.
- Um die Host-UUID unter Linux oder UNIX zu sperren, erstellen Sie eine Datei namens "/etc/calockuuid".

Standardalgorithmus (empfohlen)

Der Standardalgorithmus entdeckt sowohl IDE- als auch- SCSI-Datenträger (der Legacy-Algorithmus entdeckt nur IDE-Datenträger), und bestimmt die Änderung im Host verlässlicher als der Legacy-Algorithmus.

Nachdem der Algorithmus die Eigenschaften des Zielcomputers überprüft hat, wird in den folgenden Szenarien eine CA-spezifische UUID erstellt:

- Zusätzlich zur Seriennummer der Festplatte wurden die MAC-Adressen oder die System-ID geändert.
- Die Seriennummer der Festplatte wurde nicht gefunden. Sowohl System-ID als auch MAC-Adressen wurden geändert.

Hinweis: Bei virtuellen Rechnern verursacht eine Änderung der System-ID eine neue Host-UUID.

Legacy-Algorithmus

Sie müssen den Legacy-Algorithmus aktivieren, um ihn für die Computer-Identifizierung in CA ITCM zu verwenden.

Wichtig! Sie sollten den Legacy-Algorithmus aktivieren, bevor Sie ein Upgrade oder eine Neuinstallation durchführen. Wenn Sie den Legacy-Algorithmus nach einem Upgrade oder einer Installation ändern, wird er ungültige CA-spezifische UUIDs generieren.

Um den Legacy-Algorithmus zu aktivieren verwenden Sie je nach Betriebssystem eine der folgenden Methoden:

- Um den Legacy-Algorithmus unter Windows zu aktivieren, müssen Sie unter dem Registrierungsschlüssel "HKLM\Software\ComputerAssociates\HostUUID" einen Zeichenfolgewert "LegacyHostUUID" mit dem Wert “1” erstellen.
- Um den Legacy-Algorithmus unter Linux oder UNIX zu aktivieren, erstellen Sie eine Datei namens "/etc/calegacyuuid".

Hinweis: Sie müssen den Legacy-Algorithmus auf jedem Computer, auf dem ein CA ITCM-Agent ausgeführt wird, aktivieren.

Bei physischen Computern überprüft der Algorithmus die drei bereits beschriebenen Eigenschaften. Wenn zwei dieser drei Kriterien nicht erfüllt werden, wird das Zielsystem als neuer Computer betrachtet. Es wird eine neue CA-spezifische UUID generiert.

Wichtig! UUIDs, die von früheren Versionen der CA Technologies Desktop Management-Software generiert wurden, z. B. Unicenter® Software Delivery, Unicenter® Asset Management und Unicenter® Remote Control, sind u. U. nicht global eindeutig.

Roaming von Computern zwischen Domänen

Ein Computer kann mehreren Domänen-Managern unterstehen. Die Roaming-Funktionalität verhindert doppelte Einträge auf dem Enterprise-Manager, wenn ein Computer zwischen Domänen verschoben wird, die mit dem gleichen Enterprise-Manager verknüpft sind.

Die Informationen (also gelieferte Software, Inventarattribute usw.) von Computern, die einer anderen Domäne unterstehen, werden auf ihren neuen Domänen-Manager verschoben.

Der Computer wird in der Domäne gelöscht, aus der er übertragen wurde. Dieser Task wird standardmäßig von der Software Delivery-Funktionalität ausgeführt (wenn installiert). Wenn die Software Delivery-Funktionalität nicht installiert oder nicht darauf konfiguriert ist, Jobverläufe zu speichern, entfernt ein Replikationsjob den Computer.

Beispiel: Roaming-Computer

Die Domänen-Manager A und B sind mit demselben Enterprise-Manager verknüpft. Ein Computer X registriert sich bei Domänen-Manager A und wird mit dem Enterprise-Manager repliziert. Anschließend registriert sich Computer X bei Domänen-Manager B.

Bevor Domänen-Manager B Computer X mit dem Enterprise-Manager repliziert, prüft er, ob bereits ein Computer mit derselben UUID (d. h. einer CA Technologies-spezifischen UUID oder Host-UUID) auf dem Enterprise-Manager vorhanden ist. Er findet Computer X aus Domäne A und weiß damit, dass Computer X über Roaming von Domänen-Manager A auf Domänen-Manager B verschoben wurde. Das Konto "Domäne A/Computer X" wird auf dem Enterprise-Manager durch die Replikation von Domänen-Manager B gelöscht und in der Datenbank des Enterprise-Managers wird eine Roaming-Benachrichtigung gespeichert. Das Konto "Domäne B/Computer X" wird mit dem Enterprise-Manager repliziert. Bevor Domänen-Manager A Änderungen oder neue Computer repliziert, prüft er, ob Roaming-Benachrichtigungen vorliegen. Er findet die Benachrichtigung für Computer X und löscht ihn auf Domänen-Manager A. (Wenn auf dem Roaming-Computer ein Software Delivery-Agent installiert ist, wird er nicht sofort gelöscht.)

Computer X hat sich jetzt erfolgreich über Roaming verschoben und existiert jetzt als "Domäne B/Computer X" in der Umgebung des Enterprise-Managers.

Anpassbare Abmeldung oder Neustartbanner

Wenn Software Delivery- oder Remote Control-Funktionen eine Abmeldung oder einen Neustart des Zielcomputers initiieren, zeigt das Application Framework (CAF) ein Dialogfeld mit einer Banner-Bitmap an, in der der Benutzer über den Vorgang informiert wird.

Sie können die standardmäßige Banner-Bitmap durch eine eigene Bitmap ersetzen, indem Sie eine Bitmap-Bilddatei (mit der Dateierweiterung BMP) in der Größe 500 x 65 Pixel erstellen. Speichern Sie diese Datei auf der lokalen Festplatte oder in einer Netzwerkfreigabe, und legen Sie für die Konfigurationsrichtlinie "Allgemeine Komponenten/CAF/Allgemein/CAF-Dialogfeld: Dateiname der Bitmap" die Pfadangabe der Datei fest. Wenn das Dialogfeld angezeigt wird, liest es die Datei und zeigt das Bild an.

Verwenden eines benutzerdefinierten Reboot-Programms

Das Common Application Framework (CAF) leitet Anforderungen für den Neustart des Systems üblicherweise an das Betriebssystem weiter, das den Neustart ausführt. Es kann auch ein benutzerdefiniertes Reboot-Programm verwendet werden, in dem besondere Anforderungen berücksichtigt werden können.

Zum Aktivieren und Konfigurieren eines benutzerdefinierten Reboot-Programms stehen in der Konfigurationsrichtliniengruppe "...DSM/common/caf/general" die folgenden Einstellungen für Konfigurationsrichtlinien zur Verfügung:

CAF: Befehl zum Neustarten

Gibt es Namen des benutzerdefinierten Reboot-Programms an, das statt der API des Betriebssystems verwendet wird. Wenn kein Reboot-Programm angegeben ist, wird die API des Betriebssystems verwendet.

CAF-Dialogfeld: Dialogfeld aktivieren

Gibt an, ob ein Countdown-Dialogfeld angezeigt wird (Wert = True) oder der Neustart sofort erfolgt, ohne dass ein Countdown-Dialogfeld angezeigt wird (Wert = False). Dies ist auf speziellen Hardwaresystemen nützlich, die u. U. keine Benutzerinteraktion über ein Dialogfeld zulassen.

Dialogfeld zum Neustarten und Abmelden auf Terminalservern

Während eines Neustarts wird ein Dialogfeld angezeigt, das Sie über die durchgeführten Vorgänge und den Zeitpunkt dieser Ausführung informiert. Es enthält eine Reihe von Schaltflächen, mit denen Sie den Prozess in einem gewissen Ausmaß steuern können.

Jetzt neu starten

Startet das System unmittelbar neu, statt auf das Ablaufen des angegebenen Zeitlimits zu warten.

Zurückstellen

Verzögert den Neustart für einen gewissen Zeitraum, so dass Sie Ihre Arbeit abschließen oder speichern können.

Abbrechen

Bricht den Neustart ab.

Auf einem Computer, bei dem Sie der einzige Benutzer sind, stellt dies kein Problem dar, da nur Sie von dem Vorgang betroffen sind. Auf einem Terminalserver hingegen können mehr Benutzer betroffen sein: Eine andere Regel muss also befolgt werden. In einem solchen Fall sind sämtliche Schaltflächen deaktiviert, da durch Klicken auf eine der Schaltflächen alle Benutzer betroffen wären, ohne dass sie davon vorher in Kenntnis gesetzt würden oder dem Vorgang zustimmen könnten. Außerdem hat nur der Systemadministrator die Berechtigung, den Neustart zu steuern, da der Computer ihm oder ihr "gehört".

Beim Abmelden ist die Schaltfläche "Jetzt abmelden" allerdings aktiviert, da wieder nur Sie von diesem Vorgang betroffen sind. Die Schaltflächen "Zurückstellen" und "Abbrechen" sind nach wie vor deaktiviert.

Speicherort der Webdienste-Dokumentation und WSDL-Datei

Das *Webdienste-Referenzhandbuch* finden Sie hier:

- Im Hauptdokumentationssystem von CA IT Client Manager
- An den folgenden Speicherorten, wenn die Web-Services installiert wurden:

  http://%*Computername*%/UDSM_R11_WebService/help/index.htm (unter Windows)

  http://%*Computername*%/UDSM_R11_WebService/help (unter Linux)

Wenn die Webdienste installiert wurden, befindet sich die *WSDL-Datei* unter Windows an folgenden Speicherorten:

- http://%*Computername*%/UDSM_R11_WebService/wsdl

%*Installationsverzeichnis*%\CA\DSM\webservices\wsdl

Unter Linux befindet sich die *WSDL-Datei* an folgendem Speicherort:

- %*Installationsverzeichnis*%/CA/DSM/webservices/wsdl

Hinweise zu Webkonsolen und Webservices

Nachfolgend finden Sie die Hinweise zur Installation und Integration mit der Webkonsole und Webservices.

Für die Webkonsole benötigte Installationspakete

In der folgenden Tabelle sind die Pakete von Drittanbietern und von CA Technologies aufgelistet, die Voraussetzungen für die Webkonsole sind:

Paket	Betriebssystem	Description/Comment
AMS	Windows und Linux	CA Technologies-Komponente für Asset Maintenance System AMS wird von der Webkonsole zum Anzeigen von Informationen zu eigenen und erkannten Assets verwendet.
Apache-Webserver	Linux	Komponente, die die Webkonsolenanwendung hostet. Wenn Sie eine bestimmte Version von Apache Webserver verwenden möchten, müssen Sie die Variable CA_DSM_USE_APACHE_PROG statt auf das übergeordnete Verzeichnis auf den vollständigen Pfad der Programmdatei setzen, bevor Sie die Installation von CA IT Client Manager starten. Beispiel: CA_DSM_USE_APACHE_PROG=/apache2.2.8/bin/httpd

Paket	Betriebssystem	Description/Comment
AMS	Windows und Linux	CA Technologies-Komponente für Asset Maintenance System AMS wird von der Webkonsole zum Anzeigen von Informationen zu eigenen und erkannten Assets verwendet.
Apache Tomcat	Windows und Linux	Servlet-Container für die Webkonsole
Apache Tomcat Connector für ISAPI	Windows	Connector zwischen Internet Information Services (IIS) und Tomcat
Apache Tomcat Connector für Apache (mod_jk)	Linux (32-, 64-Bit)	Connector zwischen Apache Webserver und Tomcat
Oracle-JDBC-Treiber	Windows und Linux	Für die Verbindung zu einer Oracle-Datenbank verwendeter JDBC-Treiber.
Apache Axis	Windows und Linux	WebService-Toolkit
CA CMDB	Windows und Linux	Konfigurationsmanagement-Datenbank
CA Service Desk	Windows und Linux	
Microsoft IIS	Windows	Die Webkonsolenanwendung hostende Microsoft-Internetinformationsdienste-Komponente
Log4j	Windows und Linux	Protokollierungs-Toolkit
Microsoft SQL Server-JDBC-Treiber	Windows	Für die Verbindung zu einer SQL Server-Datenbank verwendeter JDBC-Treiber.
Microsoft SQL Server-JDBC-Treiber	Linux	Für die Verbindung zu einer SQL Server-Datenbank verwendeter JDBC-Treiber.
Sun JRE	Windows und Linux	Sun Java Runtime Environment Erforderlich für die Webkonsole bei der Verwendung von IPv6.

Wichtig! Die Änderung des SQLServer.PortNo-Schlüssels mit der Datenbank-Portnummer in der Datei "wacconfig.properties" wird nicht mehr unterstützt. Sie müssen die korrekte Portnummer während der Installation angeben. Sie kann nicht nachträglich geändert werden.

Installieren von Web Admin Console (WAC) oder Webservices auf 64-Bit-Linux-Computern

CA ITCM unterstützt den 64-Bit-Apache-Webserver auf Linux-Computern nicht. Deinstallieren Sie den 64-Bit-Apache-Webserver, bevor Sie die CA ITCM-Webkonsole oder CA ITCM-Webservices auf einem 64-Bit-Linux-Computer installieren.

Verwendung von Tomcat-Ports durch die Webkonsole

Die Webkonsole verwendet die Apache Tomcat-Web-Servlet-Engine. Als standardmäßige Tomcat-Port-Nummern werden 8090 (Starten), 8095 (Herunterfahren) und 8020 (AJP) verwendet.

Der Bildschirm mit Tomcat-Ports wird während der Installation mit Daten gefüllt. Während der Installation muss der Benutzer die richtige Port-Nummer eingeben.

Der von der Webkonsole verwendete Tomcat-Port befindet sich im Systeminstallationspfad in der Datei "server.xml".

Unter Windows befindet sich die Datei "server.xml" am folgenden Speicherort:

`[Installationspfad]\Web Console\conf\server.xml`

Unter Linux befindet sich die Datei "server.xml" am folgenden Speicherort:
`[Installationspfad]/webconsole/conf/server.xml`

Konfiguration von Tomcat-Ports für die Webkonsole

Möglicherweise sind ein oder alle der standardmäßigen Tomcat-Ports bereits von anderen CA Technologies-Anwendungen belegt, die bereits auf dem Computer installiert sind. Das Installationsprogramm der Webkonsole prüft, ob Ports bereits belegt sind und weist automatisch neue Port-Nummern zu.

Die Anwendungen, die kollidierende Port-Nummern verwenden, müssen zur Installationszeit ausgeführt werden, damit sie gefunden werden können. Wenn sie nicht ausgeführt werden, müssen Sie die Kollisionen der Port-Nummern nach der Installation manuell lösen. Wenn unterschiedliche Anwendungen versuchen, die gleichen Port-Nummern zu verwenden, starten die Anwendungen u. U. nicht. Normalerweise ist die erste gestartete Anwendung erfolgreich, und die folgenden Anwendungen schlagen fehl.

So ändern Sie die Port-Nummern, die die Webkonsole verwendet:

1. Beenden Sie die Webkonsolen-Instanz von Tomcat, wenn sie ausgeführt wird, indem Sie eine Befehlszeile öffnen und folgenden Befehl eingeben:
   ```
   caf stop tomcat
   ```
2. Öffnen Sie die Datei "server.xml" in einem Texteditor.

   Die Datei muss Einträge enthalten, die den Folgenden ähnlich sind:

   ```
   <Server port="8095" shutdown="SHUTDOWN" debug="0">
   ```

   ```
   <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
       port="8090" minProcessors="5" maxProcessors="75"
       enableLookups="true" redirectPort="8443"
       acceptCount="100" debug="0" connectionTimeout="20000"
       useURIValidationHack="false" disableUploadTimeout="true" />
   ```
3. Ändern Sie die Port-Nummern *nnnn* in den Port-Zuweisungen port="*nnnn*" (im Beispiel oben sind zwei Zuweisungen angegeben) in verfügbare, unbelegte Ports.
4. Speichern Sie die Datei, und schließen Sie den Texteditor.
5. Starten Sie die Webkonsolen-Instanz von Tomcat, indem Sie eine Befehlszeile öffnen und folgenden Befehl eingeben:
   ```
   caf start tomcat
   ```

Wenn Sie nicht sicher wissen, welche Port-Nummern von anderen Anwendungen verwendet werden, erhöhen Sie alle Port-Nummern um 1. Starten Sie anschließend die Anwendungen. Wenn weiterhin Probleme auftreten, wiederholen Sie den oben genannten Prozess.

Bereitstellung einer eigenständigen Webkonsole

Sie können die Webkonsole entweder auf dem DSM Manager-, oder auf einem anderen Computer bereitstellen. Für eine optimale Leistung empfiehlt CA, dass sich der Computer, der als Host der eigenständigen Webkonsole fungiert, und der Computer, der als Host der MDB fungiert, im selben Subnetz (am selben geographischen Standort) befinden.

Webkonsole: CMDB Viewer

Der Configuration Management Database (CMDB) Viewer (oder Visualizer) ist eine webbasierte Benutzeroberfläche, in der die Beziehung zwischen den unterschiedlichen Konfigurationselementen der CMDB-Datenbank angezeigt wird. Zwei Vorbedingungen sind, dass die CMDB auf derselben MDB wie der Domänen-Manager installiert sein muss, und dass die Konfigurationsrichtlinie "Service Desk-Integration" auf den Computer angewendet wird, auf dem WAC installiert ist.

Der CMDB-Viewer kann auf der Startseite im Abschnitt "Schnellstart" wie folgt aufgerufen werden:
Computer / Startseite / Schnellstart / Externe Anwendungen / CMDB Visualizer

Der CMDB Viewer muss separat installiert werden und ist nicht Bestandteil der CA ITCM-Installation.

Interne Abhängigkeiten

Einige DSM-Komponenten verfügen über interne Abhängigkeiten mit anderen DSM-Komponenten. Während der Installation werden die ausgewählten Komponenten auf interne Abhängigkeiten geprüft. Wenn sie von anderen DSM-Komponenten abhängig sind, werden die betreffenden Komponenten automatisch ebenfalls installiert.

Beispielsweise ist im Kontext der Software Delivery (SD)-Funktionalität für die Scalability-Server-Funktionalität ein SD-Agent auf demselben System erforderlich. Auch wenn keine Agenten für die Installation ausgewählt wurden, wird der SD-Agent automatisch installiert, wenn der Scalability-Server zur Installation ausgewählt wurde.

In den folgenden Listen werden die Abhängigkeiten dargestellt, die eine automatische Installation der zusätzlichen DSM-Komponenten zur Folge haben:

Manager:

Komponente	Erfordert ...
Manager (SD)	Alle DTS-Komponenten (Manager und Agent) auf dem gleichen System. Scalability-Server, wenn er ein Domänen-Manager ist.

Komponente	Erfordert ...
Manager (Enterprise oder Domäne)	Asset Management-Manager-Plug-in. Engine
Enterprise-Manager	DTS-Agent
Webkonsole	Webservices

Server:

Komponente	Erfordert ...
Scalability-Server (SD)	SD-Agent auf demselben System DTS-Agent

Agent:

Komponente	Erfordert ...
Katalog (SD)	SD-Agent auf demselben System

Abhängigkeiten mit anderen Produkten unter Windows.

Einige MSI-Installationspakete verfügen über Abhängigkeiten mit Produkten von Drittherstellern. Einige von ihnen installiert das CA ITCM-Installationsprogramm automatisch. Andere hingegen muss der Kunde bestellen und installieren.

CA ITCM -Installationspaket	Voraussetzungen für Programme von Drittherstellern.	Teil des Installations-Images?	Master-Setup-Installation? (*)
Explorer: Reporter-Plug-in	DB-Client	Nein	Nein
Manager: alle Plug-ins.	Für MDB: DB-Client oder lokaler DB-Server.	Nein	Nein

CA ITCM -Installationspaket	Voraussetzungen für Programme von Drittherstellern.	Teil des Installations-Images?	Master-Setup-Installation? (*)
Manager: Asset Management-Plug-in	SUN Microsystems J2SE JRE (Java Runtime Environment)	Ja	Ja: JRE ist Teil der Managerinstallation und wird während der benutzerdefinierten Installation oder durch die Installation des Managers über die MSI-Befehlszeile automatisch installiert.
Webservices	Microsoft Internet Information Server (IIS) 7.0 **Hinweis:** Die Standardinstallation von IIS 7.0 installiert nicht die für die Komponenten erforderliche Webkonsole; installieren sie ISAPI-Erweiterungen und -Filter, bevor Sie die Webkonsole installieren.	Nein	Nein

CA ITCM -Installationspaket	Voraussetzungen für Programme von Drittherstellern.	Teil des Installations-Images?	Master-Setup-Installation? (*)
Webkonsole	Apache Jakarta Tomcat 5.5.12	Ja	Ja: Tomcat ist Teil der Managerinstallation und wird während der benutzerdefinierten Installation oder durch die Installation des Managers über die MSI-Befehlszeile automatisch installiert.
	Oracle J2SE JRE 1.7.0_17 (Java Runtime Environment)	Ja	Ja: JRE ist Teil der Managerinstallation und wird während der benutzerdefinierten Installation oder durch die Installation des Managers über die MSI-Befehlszeile automatisch installiert.
	AMS 1.6.2	Ja	Ja, nur während der benutzerdefinierten Installation.

(*) Einige der Pakete, die mit "Ja" für die automatische Installation markiert sind, werden nur installiert, wenn Sie den interaktiven Installationsassistenten verwenden. Sie werden nicht installiert, wenn das MSI-Paket direkt aufgerufen wird. Dieses Verhalten hängt von der Technologie und dem Format ab, die für die dem CA ITCM-Installationsprogramm gebotenen Pakete verwendet werden.

Wenn Sie Managerkomponenten mit Software Delivery-Funktionen oder dem Bereitstellungsassistenten auf andere Systeme verteilen, müssen einige vorausgesetzte Komponenten daher zunächst manuell installiert werden, bevor das Komponentenpaket installiert wird.

Manuelle Installation von vorausgesetzten Komponenten unter Windows

Die folgenden Befehle und Vorgehensweisen sollen Sie beim Installieren der für Installationspakete vorausgesetzten Komponenten unterstützen.

- **Installieren von CA Asset Maintenance System (AMS):**

  ```
  WindowsProductFiles_x86\AMS\setupwin32console.exe -P
  installLocation="c:\Program Files\CA\DSM\Web Console\webapps\AMS" -V
  SERVERNAME="manager_system_name" -V WEBPORT="Tomcat_startup_port" -V
  DASSERVERNAME="mdb_servername" -V INGRESLISTENER="db_instance_name" -silent
  ```

- **Installieren von MSAARDK:**

  ```
  WindowsProductFiles_x86\MSAARDK\MSAARDK.exe /R:N
  ```

Wenn eine Installation über die Befehlszeile oder eine Batch-Prozedur erforderlich ist, empfehlen wir folgende Vorgehensweise: Um zu ermitteln, was installiert werden muss und welche Befehlszeilen auszuführen sind, sollten Sie eine Vorlageninstallation für diese bestimmte Kombination der Managerfunktionen ausführen. Das Installationsprogramm erstellt im Verzeichnis "%temp%" mehrere Protokolldateien. Zu diesem Befehl gelangen Sie, indem Sie "DSMSetup.log" öffnen und "Launch ciCCSSetup" suchen. Damit werden Sie zum Abschnitt der Befehle geführt, die zum Installieren der verschiedenen Komponenten ausgeführt werden.

Sie können weitere Suchvorgänge für "Launch" ausführen. Damit wird die Reihenfolge der msiexec-Befehle zur Installation der folgenden Komponenten dargestellt:

- AMS
- Agenten
- Scalability-Server
- DSM-Explorer
- Manager
- und so weiter.

In jeder Befehlszeile werden die Eigenschaften angezeigt, die beim Aufrufen des Befehls verwendet werden und die in das Automatisierungsskript kopiert werden können. Alle wichtigen Parameter werden im Abschnitt Installationstool msiexec (siehe Seite 173) erläutert.

Wenn es sich um die Installation eines Managers handelt, muss die MDB als erstes Paket installiert und konfiguriert werden, bevor eine andere Installation folgt.

Abhängigkeiten mit anderen Produkten unter Linux und UNIX

In den Linux- und UNIX-Versionen von CA IT Client Manager sind Komponenten von Drittherstellern (z. B. Java Runtime Environment) in den DVD-Images als PIF- oder RPM-Pakete eingebettet und werden entsprechend installiert, wenn ein DSM-Paket installiert wird. Normalerweise sind keine besonderen manuellen Installationsschritte erforderlich.

In einigen Linux-Versionen müssen jedoch Laufzeit-Kompatibilitätsbibliotheken installiert werden, bevor Sie die DSM-Komponenten installieren. Weitere Angaben finden Sie im Abschnitt Kompatibilitätsbibliotheken für Linux.

Für die Taskleiste muss unter Linux das GIMP-Toolkit GTK+ 1.2 (genau diese Version) installiert sein. Das GTK ist nicht im Lieferumfang von CA IT Client Manager enthalten. Sie müssen die erforderliche Version unter www.gtk.org herunterladen.

Während der Installation in Linux und UNIX steht eine umfassende Kontrolle der Paketauswahl zu Verfügung, in der die Antwortdateieinstellungen in Verbindung mit der Befehlszeilenoption "/R" für den Installationsbefehl verwendet werden. Umfassende Informationen zu den verfügbaren Optionen finden Sie unter Installation von CA ITCM über die Befehlszeile in Linux und UNIX (siehe Seite 194).

Neustarten von Apache unter Linux

Wenn Sie Apache neu starten müssen, tun Sie dies nicht über eine Linux-GUI, da diese die für CA IT Client Manager erforderliche Umgebung nicht berücksichtigt. Stattdessen können Sie z. B. zu einer Shell wechseln und Apache dort mit folgendem Befehl starten:

```
dsm_restart_apache [-f]
```

Wenn Apache noch nicht ausgeführt wird, wird es mit der Option "-f" gestartet.

Wenn Sie die Option "-f" nicht angeben und Apache nicht ausgeführt wird, wird Apache nicht gestartet. Wenn Apache bereits ausgeführt wird, erfolgt ein Neustart.

Kapitel 3: Installation von CA ITCM

Das folgende Kapitel enthält Informationen zum allgemeinen Prozess und zu den Anforderungen für die Installation von CA ITCM. Sie können die Abschnitte am Anfang des Kapitels überspringen, die sehr spezielle Hinweise und Informationen zur Installation von DSM-Komponenten enthalten, und die Einführung zum Installer und zum Installationsprozess lesen. Es folgen Beschreibungen der interaktiven Installation und der Installation über die Befehlszeile.

Dieses Kapitel enthält folgende Themen:

Funktionsweise des Installationsprozesses (siehe Seite 106)
Einführung in den Installer (siehe Seite 106)
Voraussetzungen und Einschränkungen (siehe Seite 107)
Installationsmethoden (siehe Seite 107)
Installationshinweise (siehe Seite 108)
Installationshinweise zu FIPS (siehe Seite 110)
Während Installation den FIPS-Modus auswählen (siehe Seite 110)
Installieren der automatisierten Migration (siehe Seite 112)
Mehrsprachige Installation (siehe Seite 113)
Informationen zur Erstellung und Installation von Agenten-Sprachpaketen (siehe Seite 114)
Erforderliche Hardwarekonfiguration (siehe Seite 115)
Management-Datenbank (MDB) (siehe Seite 116)
Besondere Hinweise zu CA ITCM-Installationen (siehe Seite 140)
Administrative Installation unter Windows (siehe Seite 158)
Installationsverzeichnisse unter Windows (siehe Seite 159)
Installationsverzeichnisse unter Linux und UNIX (siehe Seite 160)
Installieren des Alarm-Collector (siehe Seite 161)
Einschränkungen für Computer-, Benutzer- und Verzeichnisnamen (siehe Seite 162)
Interaktive Installation mit dem Installationsassistenten (siehe Seite 164)
Installation von CA ITCM über die Befehlszeile in Windows (siehe Seite 170)
Installation von CA ITCM über die Befehlszeile in Linux und UNIX (siehe Seite 194)
Installationsprotokolldateien (siehe Seite 209)
Versionsinformationen zu installierten DSM-Komponenten (siehe Seite 210)

Funktionsweise des Installationsprozesses

Der Installationsprozess besteht aus drei Hauptschritten:

1. Vorbereitungsphase
2. Interview-Phase
3. Ausführungsphase

Während der Vorbereitungsphase informieren Sie sich über die Produktoptionen und sammeln alle erforderlichen Informationen für die Installation, wie in den ersten Abschnitten dieses Kapitels beschrieben. Sie müssen dabei vorhandene Softwarevoraussetzungen überprüfen oder fehlende installieren und die Installation anderer Produktfunktionen, die mit dem Installationsmedium ausgeliefert werden, auswählen und starten.

Während der Interview-Phase geben Sie die Informationen an, die Sie in Schritt 1 gesammelt haben, indem Sie sie auf den Seiten des Installationsassistenten angeben oder eine Antwortdatei erstellen. Beispielsweise geben Sie die Sprache der Installation und des zu installierenden Produkts, den Installationstyp (Express- oder benutzerdefinierte Installation) und wichtige Konfigurationseinstellungen zum Ausführen der installierten Komponenten an.

Schließlich führen Sie die Installationsanweisungen mit den in Schritt 2 eingegebenen Informationen aus.

Mit dem Installationsassistenten können Sie Produktkomponenten interaktiv installieren und entfernen. Darüber hinaus können in einer Befehlszeilenoberfläche zahlreiche Installations- und Konfigurationsparameter angegeben und geändert werden.

Einführung in den Installer

Der CA ITCM-Installer bietet Installationsroutinen für die Installation von grundlegenden Produktfunktionen und optional von weiteren CA Technologies-Produkten in Form von Plug-ins.

Verfügbar sind die Optionen zur Express-Installation und zur benutzerdefinierten Installation. Die Express-Installationen bieten die schnelle Verfügbarkeit einiger Management-Funktionen, während die Option für die benutzerdefinierte Installation eine größere Flexibilität und differenziertere Möglichkeiten zur Auswahl von Funktionen zur Verfügung stellt.

Sie können die erworbenen Produktfunktionalitäten auswählen und mit einer Express-Installation oder einer benutzerdefinierten Installation fortfahren. Alle Benutzer haben die Option, Produktfunktionen auszuwählen, für die sie noch keine Lizenz erworben haben, und diese 30 Tage lang zu testen.

Voraussetzungen und Einschränkungen

Beachten Sie bei der Installation von CA ITCM Version 12.8 die folgenden Voraussetzungen und Einschränkungen:

- Ihr Datenbankprovider muss Microsoft SQL Server oder Oracle sein.
- Bei Oracle muss bei der Managerinstallation das "sys"-Kennwort des Datenbankadministrators während des Installer-Interviews eingegeben werden. Bei SQL Server sind die Felder DB-Administrator und DB-Administratorkennwort ausgeblendet. Zur Installation der MDB und zur Einrichtung des DSM-Managers verwendet das Installationsprogramm eine vertrauenswürdige SQL Server-Verbindung.

Installationsmethoden

Wenn Sie die zu installierenden Produktfunktionen ausgewählt haben, können Sie die Installationsmethode auswählen und die Eingabeaufforderungen durchlaufen, um die Verteilung und Konfiguration des Produkts zu starten.

Die folgenden Installationsmethoden stehen zur Verfügung:

Express-Installation

Installiert einen eigenständigen Domänen-Manager mit Scalability-Server, Agent und DSM-Explorer unter Windows.

Express-Agent-Installation

Installiert alle Funktionen, die zur Verwaltung eines Endsystems erforderlich sind. Im Idealfall sollte der Domänen-Manager oder Scalability-Server, der dieses Endsystem verwaltet, bereits im Netzwerk installiert worden sein.

Benutzerdefinierte Installation

Hier können Sie einzelne Produktkomponenten auswählen oder ihre Auswahl aufheben und die Installationseinstellungen ändern.

Installationshinweise

Die folgenden Hinweise gelten, wenn Sie eine MDB auf Oracle 11g installieren möchten:

- Es muss mindestens ein Oracle 11g-Client installiert sein.
- Wenn Sie bei der Installation eines DSM-Managers mit einer Oracle-MDB auswählen, eine CCS-Komponente zu installieren, müssen Sie über ein C:-Laufwerk verfügen und dürfen den standardmäßigen Installationspfad der CCS-Komponente nicht ändern.
- CA ITCM unterstützt nur die EZCONNECT-Verbindungsmethode vom DSM-Manager zur Oracle-Datenbank. Weitere Informationen zur Einstellung der Verbindungsmethode EZCONNECT finden Sie in der Oracle-Dokumentation.
- Der DSM-Manager kann nicht auf demselben Computer wie der Oracle 11g-Server (64 Bit) oder -Client installiert werden, da er den Oracle 11g-Client (32 Bit) benötigt. Wenn die MDB auf einem Oracle 11g-Server (64 Bit) installiert wird, muss dieser Server remote vom DSM-Manager sein.
- Sowohl IPv4 als auch IPv6 werden zwischen dem DSM-Manager und der MDB unterstützt.
- Ein Minimum von 2 GB wird sowohl für System Global Area (SGA) als auch für Program Global Area (PGA) empfohlen.
- Das Installationsprotokoll befindet sich im temporären Verzeichnis und heißt "mdb-schema-setup.log".
- Geben Sie die richtigen "sys"-, "mdbadmin"- und ca_itrm"-Kennwörter bei einer Neuinstallation oder einem Upgrade an.
- Das MDB PIF-Paket unterstützt die unbeaufsichtigte Installation von einer Antwortdatei unter Windows und Linux/Solaris.
- Wenn die zugrunde liegende Datenbank Oracle ist, geben Sie die "mdbadmin"-Anmeldeinformationen an, um eine Verbindung zur Datenquelle herzustellen. Fügen Sie "mdbadmin" außerdem die AIADMIN-Rolle hinzu, bevor Sie die Extrahierung ausführen.
- Stellen Sie sicher, dass JRE 1.7 auf dem Windows-Computer vorhanden ist, auf dem Sie die MDB-Admin-Konsole installieren möchten. Stellen Sie außerdem sicher, dass die Umgebungsvariable "JAVA_HOME" festgelegt ist und auf den JRE-Installationsordner zeigt.
- Die MDB-Admin-Konsole verwendet eine Hibernate-Technologie für den Zugriff auf MDB-Objekte. Laden Sie Hibernate 3.2.0 unter http://sourceforge.net/projects/hibernate/files/ herunter, und stellen Sie es auf dem Computer zur Verfügung, auf dem Sie die MDB-Admin-Konsole verwenden möchten.

Weitere Informationen:

Installationsvoraussetzungen (siehe Seite 112)

Verschiedene Installationshinweise

Wenn Windows-Terminaldienste wird im Anwendungsservermodus konfiguriert sind, sind die folgenden Einstellungen erforderlich:

- Verwenden Sie den Modus "CONSOLE", wenn Sie die Installation über einen Remotezugriff ausführen.
  Beispiel:

  mstsc /v:HostName /console

- Ändern Sie vor der Installation die Terminalserver-Benutzereinstellungen auf "INSTALL".
  Beispiel:
  change user /install

- Führen Sie den folgenden Befehl aus, um die Benutzereinstellungen zu überprüfen:
  `change user /query`

Hinweis: Weitere Informationen zum Hilfsprogramm CHANGE USER des Windows-Terminalservers finden Sie unter Support. microsoft.com/kb/186504.

Weitere Informationen:

Installationsvoraussetzungen (siehe Seite 112)

Installationshinweise zu FIPS

Die folgenden Installationsüberlegungen gelten, wenn Sie CA ITCM in einem der FIPS-Modi installieren:

- Alle DSM-Komponenten auf einem Computer verwenden dem gleichen FIPS-Modus. Wenn Sie zum Beispiel einen Asset Management-Agenten auf einem Computer installieren, der schon über den Version 12.8-Software-Delivery-Agenten verfügt, werden beide im gleichen FIPS-Modus funktionieren.
- Alle Managerkomponenten, wie Engine, Webdienste, Webkonsole, und Reporter muss den gleichen FIPS-Modus verwenden, den der Manager verwendet.
- In geclusterten Bereitstellungen können Sie den FIPS-Modus nur für den ersten Knoten auswählen; alle anderen Knoten funktionieren im gleichen Modus wie der erste Knoten.

Während Installation den FIPS-Modus auswählen

Sie können den FIPS-Modus auswählen, wenn Sie CA ITCM interaktiv mit dem Installationsprogramm oder automatisch über die Befehlszeile, msiexec oder Infrastrukturbereitstellung (DMDeploy) installieren. "FIPS-bevorzugt" ist der Standardmodus.

Hinweis: Sie können den FIPS-Modus nicht angeben, wenn Sie eine CA ITCM-Installation ändern oder diese reparieren. Wenn Sie den FIPS-Modus der DSM-Komponenten nach Installation ändern möchten, wechseln Sie in den erforderlichen Modus. Weitere Informationen zum Wechsel in einen spezifischen FIPS-Modus finden Sie im Abschnitt zu den Sicherheitsfunktionen.

Dieser Abschnitt beschreibt, wie Sie den FIPS-Modus ändern können, wenn Sie verschiedene Installationsmethoden und Optionen verwenden:

Interaktive Installation

Das CA ITCM-Installationsprogramm bietet eine Option für die Auswahl des FIPS-Modus im Abschnitt "FIPS-Compliance", wenn Sie das Produkt installieren. Aktivieren Sie das Kontrollkästchen, um den Modus "Nur-FIPS" für die Komponenten zu aktivieren, die Sie installieren. Das Installationsprogramm bietet diese Option nicht, wenn Sie eine Installation ändern oder reparieren.

Hinweis: Sie können den FIPS-Modus nur während einer benutzerdefinierten Installation auswählen. Express-Installation installiert immer CA ITCM im Modus "FIPS-bevorzugt". Für eine eigenständige Remote Control-Agent-Installation können Sie sowohl bei der benutzerdefinierten als auch bei der Express-Installation den FIPS-Modus angeben.

Installation unter Verwendung der Befehlszeile, msiexec oder DMDeploy

Sie können den folgenden Parameter angeben, um den FIPS-Modus festzulegen, wenn Sie eine automatische Installation unter Verwendung der Befehlszeile, msiexec oder DMDeploy ausführen:

Windows:

```
FIPS_MODE=1 //(FIPS-bevorzugt)
FIPS_MODE=2 //(Nur-FIPS)
```

Linux oder UNIX:

```
/RITCM_FIPS_MODE=1 //(FIPS-bevorzugt)
/RITCM_FIPS_MODE =2 //(Nur-FIPS)
```

Hinweis: Der Parameter "FIPS-Modus" wird ignoriert, wenn Sie eine vorhandene DSM-Komponente ändern oder aktualisieren oder eine zusätzliche -DSM-Komponente auf dem Ziel installieren. Im ersten Fall wird der FIPS-Modus auf "FIPS wird bevorzugt" festgelegt; im letzteren Fall entspricht der FIPS-Modus der neuen Komponente der der vorhandenen Komponente.

Installation mit Software Delivery

Sie können den FIPS-Modus nicht angeben, wenn Sie Software Delivery verwenden, um DSM-Komponenten zu installieren oder ein Upgrade durchzuführen. Die Entscheidung für einen FIPS-Modus basiert auf den folgenden Faktoren:

- Wenn das Ziel bereits eine installierte DSM-Komponente aufweist, verwendet jede weitere Installation durch Software Delivery den gleichen FIPS-Modus wie die vorhandene Komponente. Sonst wird der FIPS-Modus festgelegt auf "FIPS-bevorzugt".
- Wenn Sie das Upgrade einer DSM-Komponente durchführen, wird der FIPS-Modus als "FIPS-bevorzugt" festgelegt, wie bei jeder anderen Komponente, für die eine Upgrade durchgeführt wurde.
- Sie können den FIPS-Modus nicht angeben, wenn Sie eine CA ITCM-Installation ändern oder diese reparieren.

In allen Fällen kann sich der Manager über den FIPS-Modus hinwegsetzen, indem er die Konfigurationsrichtlinie anwendet, die den FIPS-Modus festlegt.

Weitere Informationen:

Zusätzliche Eigenschaften für msiexec (siehe Seite 191)
MSI-Eigenschaften für das Scalability-Server-Paket (siehe Seite 183)
Manuelle Installation der Primer-Software für Infrastructure Deployment (siehe Seite 253)
Grundlegende Installationseigenschaften (siehe Seite 197)
Eigenschaften des SD-Boot-Servers (nur Linux) (siehe Seite 206)
Übergabe von Optionen an die DMPrimer-Installation (siehe Seite 251)
Bereitstellung der Agentenpakete (siehe Seite 255)

Installieren der automatisierten Migration

Installationsvoraussetzungen

Überprüfen Sie, ob die folgenden Installationen in Ihrem Unternehmen verfügbar sind, bevor Sie mit der Installation beginnen:

- CA IT PAM Version 03.0.00 und Service Pack 03.0.01 oder CA Process Automation 03.1.00 und Service Pack 03.1.01 oder CA Process Automation 4.1 SP1.

  Hinweis: Sie können alternativ CA EEM für die Identitäts- und Zugriffsverwaltung installieren. Wenn Sie CA EEM in einer Windows-64-Bit-Umgebung installieren möchten, folgen Sie den Anweisungen in der Datei *EEM_Install_64.pdf* vor der Installation.

- Wenn Sie Oracle MDB und CA IT PAM Version 03.0.00 verwenden, müssen Sie den CA IT PAM-Patch ITPAM_3.0_11182010_OracleJar_HF_19813962 in Ihrer CA IT PAM-Installation installieren.

  Wichtig! Halten Sie den CA IT PAM-Orchestrator-Dienst an, bevor Sie den Patch anwenden.

Installationshinweise

Die folgenden Hinweise gelten für die automatische Migration:

- Die automatische Migration unterstützt DSM-Domänenmanager und kann daher nicht auf DSM-Enterprise-Manager angewandt werden.
- Die automatische Migration gilt nur für den mit der Webkonsole verbundenen standardmäßigen Domänen-Manager. Wenn die Webkonsole mit mehreren Domänen-Managern verbunden ist, ist die automatische Migrationsfunktionalität nur verfügbar, wenn eine Verbindung zum standardmäßigen Domänen-Manager vorhanden ist.
- Die automatische Migration kann nur auf einer Webkonsoleninstanz pro Domänen-Manager installiert werden. Wenn mehrere Webkonsoleninstanzen über denselben standardmäßigen Manager verfügen, dürfen Sie die automatische Migration nur auf einem der Webkonsolencomputer installieren.
- Die automatische Migration wird in Windows-Betriebssystemumgebungen unterstützt.
- Wenn Sie die automatische Migration ändern oder deinstallieren, wenn der WAC Manager auf einem Remote-Computer installiert ist, müssen Sie sicherstellen, dass CAF aktiviert ist.

Konfigurieren der automatisierten Migration

Um automatisierte Migration verwenden zu können, schließen Sie die folgenden Tasks ab:

1. Konfigurieren des CA IT PAM-Benutzerkontos in CA ITCM
2. Aktivieren von SSL für Webkonsole und Automatisierungs-Webservices
3. (Optional) Ändern der Automatisierungsdienst-Konfigurationsdatei

Hinweis: Weitere Informationen finden Sie unter Automatisierungsdienst-Konfigurationsdatei (siehe Seite 545).

Mehrsprachige Installation

Zu Beginn einer CA ITCM-Installation wird ein Dialogfeld angezeigt, in dem Sie die Sprache für die Installation auswählen können. Wenn die lokale Installationsumgebung in einer der unterstützten Sprachen vorliegt, ist diese Sprache bereits als Standardsprache ausgewählt. Wenn Sie eine andere Sprache auswählen, wird der Installer in der ausgewählten Sprache ausgeführt.

Für mehrsprachige Installationen von CA IT Client Manager befinden sich auf dem Installationsmedium (DVD) neben der englischen Originalversion auch andere Sprachversionen des Produkts.

Die Sprache, die Sie für die Ausführung des Installers auswählen, ist nicht notwendigerweise dieselbe Sprache, in der auch das Produkt ausgeführt wird. Während der Installation werden Sie aufgefordert, die Sprachen auszuwählen, in der das Produkt ausgeführt werden soll, sowie die Sprachen, die in den Software Delivery- und Infrastructure Deployment-Softwarebibliotheken für das Produkt verfügbar gemacht werden sollen.

Unabhängig von der Sprache, die Sie für die Installation von CA ITCM ausgewählt haben, wird CA Common Services (CCS) stets in Englisch angezeigt.

Wenn keine Spracheinstellung angegeben wird (bei einer unbeaufsichtigten Installation), wird das Standardgebietsschema des Systems verwendet, sofern ein entsprechendes Sprachpaket verfügbar ist. Wenn es sich bei dem Standardgebietsschema des Systems um keine der unterstützten Sprachen handelt, verwendet der Installer standardmäßig Englisch (USA).

Wichtig! Es ist erforderlich, dass die zugrunde liegende Domänennamen-System-Infrastruktur (DNS) die UTF-8-Zeichenkodierung in DNS unterstützt, um lokalisierte Hostnamen, d. h. Hostnamen in anderen Sprachen als Englisch, zu unterstützen.

Weitere Informationen:

Ändern der Produktsprache nach der Installation (siehe Seite 211)

Informationen zur Erstellung und Installation von Agenten-Sprachpaketen

CA IT Client Manager stellt sprachunabhängige Basispakete für den BHI-Agenten (Basis-Hardware-Inventar), den AM-Agenten (Asset Management), den RC-Agenten (Remote Control) und den SD-Agenten (Software Delivery) zur Verfügung. Diese Basispakete enthalten bereits das englische Sprachpaket (ENU), weshalb es kein separates ENU-Paket gibt.

Administratoren können Ihren eigenen Satz an Agentenpaketen mit Hilfe des dsmPush-Skripts erstellen und die jeweilige Sprache für die einzelnen Agenten angeben. Dies muss über den Manager-Computer bei im Laufwerk eingelegter DVD durchgeführt werden.

Das dsmPush-Skript erstellt installierbare Einheiten, die ein sprachunabhängiges Basispaket für eine Agentenrolle sowie die gewünschten Sprachpakete enthalten. Falls in der Befehlszeile angegeben, importiert dsmPush diese installierbaren Einheiten in die Software Delivery- oder Infrastructure Deployment-Bibliotheken. Wird dsmPush zusammen mit dem Parameter "-single" verwendet, kann der Administrator erzwingen, dass nur ein einziges Paket in die Bibliotheken importiert wird.

Ein Sprachpaket kann gleichzeitig mit dem Basispaket oder zu einem späteren Zeitpunkt gesondert installiert werden. Die Installation eines Sprachpakets wird vollkommen automatisch durchgeführt.

Wir empfehlen, die Sprachpakete mit Hilfe des dsmPush-Skripts in Software Delivery und Infrastructure Deployment zu registrieren.

Hinweis: Ausführliche Informationen zum Tool "dsmPush" finden Sie im *CLI-Referenzhandbuch*.

Bei der Agenteninstallation werden keine Pakete in die Infrastructure Deployment-Bibliothek importiert, sondern lediglich der Agent und (sofern es sich nicht um eine ENU-Installation handelt) ein Sprachpaket werden installiert. Sind jedoch bereits mehrsprachige Agentenpakete vorhanden, aktualisiert der Installer die mehrsprachigen Agenten, ohne ein Sprachpaket zu installieren.

Die interaktive Installation bietet eine Auswahl an verschiedenen Sprachpaketen, die installiert werden können und in denen das Produkt ausgeführt wird. Diese werden außerdem in die Software Delivery- und Infrastructure Deployment-Softwarebibliotheken importiert.

Installationsszenarien für bestimmte Agenten

Die folgende Liste enthält relevante Informationen zu Installations- und Aktualisierungsszenarien für bestimmte Agenten:

- **Agentenprozeduren auf Gesamtpaketen**

  Wenn mit dem Skript "dsmPush" Gesamtpakete erstellt werden, die aus einem oder mehreren Agentenbasis- und Sprachpaketen bestehen, sind die einzig verfügbaren Prozeduren für das Gesamtpaket in der Software-Paket-Bibliothek (angezeigt im DSM-Explorer unter *Domäne*, Software, Software-Paket-Bibliothek, Software-Pakete, *Paket*, Prozeduren) die Installation für Linux sowie die Installation und Deinstallation für Windows.

  Wenn Sie eine produktspezifische Aktion, beispielsweise die Prozedur für einen SWD-Scan des Software Delivery-Agenten (SD), durchführen möchten, führen Sie die Prozedur über das sprachunabhängige Basispaket des SD-Agenten in der Software-Paket-Bibliothek aus.

- **Installation eines eigenständigen Remote Control-Agenten**

  Ein eigenständiger Remote Control-Agent (RC) kann nicht mit SD-Funktionen installiert werden, da hierzu bereits ein SD-Agent auf dem Agenten-Host vorhanden sein muss. (Außerdem muss ein RC-Agent tatsächlich eigenständig sein, er darf nicht zusammen mit anderen Agenten-Plug-ins vorkommen.)

  Die Installation eines eigenständigen RC-Agenten kann nur interaktiv oder über den Infrastructure Deployment-Assistenten unter Angabe des zusätzlichen Parameters /RITRM_RC_AGENT_STANDALONE=1 erfolgen. Daher ist die RC-Agentenprozedur für eigenständige Agenten in Bezug auf Gesamtpakete in der Software-Paket-Bibliothek nicht relevant.

Erforderliche Hardwarekonfiguration

Die Hardware-Spezifikationen hängen von zahlreichen Parametern ab, einschließlich der Netzwerkarchitektur, der verfügbaren Bandbreiten, der Häufigkeit von Operationen, der Größe von Operationen und der Anzahl der Endsysteme. Wenn Sie z. B. einen Software Delivery-Manager installieren, hängt die erforderliche Speicherkapazität auf der Festplatte überwiegend von der Größe und Anzahl der verwalteten Softwarepakete und OSIM-BS-Images ab.

Im Kapitel "Hardwarespezifikationen und -anforderungen" der *CA IT Client Manager-Readme-Datei* sind die Hardwareanforderungen beschrieben, die mindestens erfüllt werden müssen, damit CA IT Client Manager ordnungsgemäß installiert und ausgeführt werden kann.

Management-Datenbank (MDB)

Der DSM-Manager erfordert eine Management-Datenbank (MDB). Die aktuelle Liste unterstützter Plattformen finden Sie auf der Website des CA Supports in der Kompatibilitätsmatrix.

MDBs können in den folgenden Konfigurationen vorkommen:

- **Lokale Konfiguration** – Der Manager und die Datenbank werden auf demselben Computer ausgeführt.

  In CA IT Client Manager gilt dies nur für eine MDB, die auf Microsoft SQL Server basiert. Der Manager und die MDB sind beide in einer Windows-Betriebsumgebung installiert.

- **Remote-Konfiguration** – Die Datenbank befindet sich auf Computer A, und der Manager ist auf Computer B installiert und verwendet einen Client, um eine Verbindung zu der Datenbank auf Computer A herzustellen.

  In CA IT Client Manager gilt dies für Microsoft SQL Server- und Oracle-MDBs.

  Für eine Oracle-MDB ist die Remote-Konfiguration obligatorisch. Tatsächlich befindet sich der DSM-Manager auf einem Computer, auf dem Windows ausgeführt wird, und die Oracle-MDB ist auf einem Computer installiert, auf dem ein unterstütztes Sun Solaris-Betriebssystem ausgeführt wird.

In der Multi-Tier-Architektur können Instanzen der Management-Datenbank (MDB) auf der Enterprise- und der Domänen-Manager-Ebene implementiert werden. Auf beiden Ebenen werden Microsoft SQL Server- und Oracle-MDBs unterstützt. Sie können zudem MDBs unterschiedlicher Datenbank-Provider auf den verschiedenen Ebenen implementieren, z. B. können Sie SQL Server als Domänen-Manager und Oracle als Enterprise-Manager auswählen..

In gemischten Konfigurationen, z. B. bei einem Domänen-Manager mit SQL Server-basierter MDB und einem Enterprise-Manager mit Oracle-basierter MDB, benötigen Sie die entsprechenden Datenbank-Clients auf den Managern. In diesem Beispiel wären dies der Oracle-Client auf dem Domänen-Manager und der SQL-Client auf dem Enterprise-Manager.

Bevor die Installation von CA IT Client Manager startet, muss entweder der Datenbankserver (für die lokale Konfiguration) oder der Datenbank-Client (für die Remote-Konfiguration) installiert werden.

Während der Installation von CA IT Client Manager wählen Sie den Datenbanktyp aus.

MDB-PIF-Paket

Sie können das Paket als ein eigenständiges MDB-Installationsprogramm verwenden.

Eigenständige MDB-Installation

Sie können das MDB-PIF-Paket als ein eigenständiges MDB-Installationsprogramm aufrufen, indem Sie das Setup-Skript (setup.bat oder setup.sh) über das entsprechende MDB-Verzeichnis ausführen:

```
<DVDROOT>\WindowsProductFiles_x86\mdb
```

```
<DVDROOT>/LinuxProductFiles_x86/mdb
```

```
<DVDROOT>/SolarisProductFiles_sparc/mdb
```

Das MDB-PIF-Paket als ein eigenständiges Installationsprogramm unterstützt neue MDB-Installationen, Neuinstallationen und Upgrades für einen lokalen oder einen Remote-Zieldatenbankserver.

Für Oracle: Das eigenständige MDB-PIF-Paket testet, ob sich der Oracle-Client auf Oracle 11g Release 2-Ebene befindet.

Weitere Informationen:

Remote-MDB-Installation für Oracle (siehe Seite 136)
Installieren einer Oracle-MDB (eigenständig) (siehe Seite 131)
Installieren des DSM-Managers: Oracle-MDB (siehe Seite 133)
Installieren des DSM-Managers: Microsoft SQL Server-MDB (siehe Seite 127)
Unbeaufsichtigte MDB-Installation mithilfe einer Antwortdatei (siehe Seite 124)
Remote-MDB-Installation für Microsoft SQL Server (siehe Seite 128)

PIF-Installationsdaten

Das MDB-Installationsprogramm hinterlässt keine PIF-Installationsdaten auf dem aufgerufenen Quellcomputer. Dadurch können Sie den Quellcomputer wieder verwenden, um die MDB auf einem anderen Ziel-Remote-Computer zu installieren. Auf Letzteren verbleiben keine PIF-Installationsdaten.

Das MDB-Installationsprogramm schreibt jedoch zur Wartungsunterstützung seine Versionsnummer in die Tabelle "ca_settings".

Alte PIF-Installationsdaten auf dem Remote-MDB-Computer werden bei einem MDB-Upgrade nicht entfernt, und zwar unabhängig davon, ob dies lokal oder remote erfolgt. Sie können diese alten Installationsdaten manuell unter Solaris mit dem folgenden Befehl entfernen: lsm -e.

Hinweise zu CCS

Mit CA IT Client Manager werden zwei Varianten von CA Common Services (CCS) installiert: eine eingeschränkte Version, genannt Micro-CCS (nur Englisch), und die ursprüngliche Vollversion. Micro-CCS (nur Englisch) unterstützt Event Management und Kalender, jedoch nicht WorldView (für die DTS-Netzwerkkonfiguration) und Discovery (einschließlich Continuous Discovery). Die Vollversion von CCS r11.2 (nur Englisch) kann nur mit einer Microsoft SQL Server-MDB verwendet werden.

Der Installer wählt während der Installation automatisch die geeignete Variante aus. Beachten Sie, dass die Varianten nicht auf einem Host gemeinsam vorhanden sein können, jedoch auf verschiedenen Hosts innerhalb eines Netzwerks. Beachten Sie ebenfalls, dass kein Upgrade von Micro-CCS auf die Vollversion von CCS möglich ist.

In den folgenden Tabellen ist zusammenfassend dargestellt, welche Variante von CCS zusammen mit den verschiedenen Betriebsumgebungen und MDBs installiert wird:

Linux:

Installierte Komponente	CCS-Variante
Agent	Keine
Scalability-Server ohne Kalender	Keine
Scalability-Server mit Kalender	Micro-CCS; nur Ereignisagent

Hinweis: CA IT Client Manager verwendet unter Linux nie die Vollversion von CCS.

Windows:

Installierte Komponente	CCS-Variante
Agent	Keine
Scalability-Server ohne Kalender	Keine
Scalability-Server mit Kalender	Micro-CCS; nur Ereignisagent
*Manager mit lokaler SQL Server-MDB	CCS-Vollversion
*Manager mit Remote-SQL Server-MDB	CCS-Vollversion; muss auf MDB-Host installiert sein, sollte auch auf CA ITCM-Host installiert sein
*Manager mit Remote-Oracle-MDB	Nur Micro-CCS auf CA ITCM-Host; Ereignisagent plus Ereignis-Manager

* Es spielt keine Rolle, ob Clustering verwendet wird.

UNIX:

Es wird keine Variante von CCS installiert.

Hinweis: Bei der Installation eines Domänen-Managers mit CCS führt die Verwendung einer benannten SQL Server-Instanz dazu, dass die CCS-Installation fehlschlägt. Zur erfolgreichen Installation von CCS mit Hilfe einer benannten SQL-Instanz muss der SQL Server-Browser-Dienst ausgeführt werden. Sie können den SQL Server-Browser-Dienst aus dem SQL Server-Konfigurations-Manager heraus starten.

CCS-Installationsfehlermeldungen

Beachten Sie, dass die Installation von CCS-Kalendern nur mit einem Scalability-Server zuverlässig ist. Die folgenden Meldungen können auftreten, wenn die Installation der *Vollversion* von CCS mit einem DSM-Manager ausgeführt wird. Alle hier aufgeführten Fehler beziehen sich auf die Interaktion zwischen CCS und einer SQL Server-basierten MDB.

Fehlertext (in %TEMP%\ TRC_Inst2_ITRM.log)	Bedingungen	Diagnosen und Maßnahmen
Der MSSQL-Server wird nicht auf \\local_host ausgeführt.	Die MDB ist remote; lokale und Remote-Hosts befinden sich nicht in derselben Domäne.	Diese Meldung ist irreführend, da kein Kontakt zum Remote-MDB-Host hergestellt wird. Fügen Sie den lokalen Host zur selben Domäne hinzu wie den Remote-Host.

Fehlertext (in %TEMP%\ TRC_Inst2_ITRM.log)	**Bedingungen**	**Diagnosen und Maßnahmen**
Der MSSQL-Server wird nicht auf \\local_host ausgeführt.	Die MDB ist remote; lokale und Remote-Hosts befinden sich nicht in derselben Domäne.	Diese Meldung ist irreführend, da kein Kontakt zum Remote-MDB-Host hergestellt wird. Fügen Sie den lokalen Host zur selben Domäne hinzu wie den Remote-Host.
Das für den nsmadmin-Benutzer eingegebene Kennwort ist ungültig.		■ Das nsmadmin-Konto war bereits in SQL Server vorhanden, und bei der DSM-Installation wurde ein anderes Kennwort angegeben. Sie können entweder (a) alle DSM/CCS-Anmeldungen und DB-Benutzer von SQL Server löschen, bevor Sie die Installation starten, (b) bei der DSM-Installation ein übereinstimmendes Kennwort angeben oder (c) das nsmadmin-Kennwort in SQL Server dahingehend ändern, dass es mit dem bei der DSM-Installation angegebenen Kennwort übereinstimmt. ■ Das nsmadmin-Kennwort erfüllt nicht die Sicherheitskriterien für das Systemkennwort. Wählen Sie ein sichereres Kennwort.
Die übermittelten MDB-Anmeldeinformationen sind nicht gültig.		Das nsmadmin-Konto wurde für SQL Server bereits definiert; die MDB selbst ist vorhanden oder auch nicht. Diese Meldung wird auch dann angezeigt, wenn das nsmadmin-Kennwort mit dem bereits in SQL Server festgelegten Kennwort übereinstimmt. Löschen Sie die DSM/CCS Anmeldung(en) und DB-Benutzer aus SQL Server, damit dort keine derartigen Daten mehr vorhanden sind.

Fehlertext (in %TEMP%\ TRC_Inst2_ITRM.log)	**Bedingungen**	**Diagnosen und Maßnahmen**
Der MSSQL-Server wird nicht auf \\local_host ausgeführt.	Die MDB ist remote; lokale und Remote-Hosts befinden sich nicht in derselben Domäne.	Diese Meldung ist irreführend, da kein Kontakt zum Remote-MDB-Host hergestellt wird. Fügen Sie den lokalen Host zur selben Domäne hinzu wie den Remote-Host.

Aktive Prozesse sind mit einer oder mehreren Datenbanken verbunden, die von diesem Produkt verwendet werden. Beenden Sie diese Vorgänge, um die Datenbankverbindungen zu schließen, bevor Sie mit der Installation beginnen; dies dient dem Erhalt der Datenintegrität und der Systemstabilität.
[In %TEMP%\ITRM.CCS\wizint.log oder %TEMP%\DSM_CCS_wizint.log.]
		Die MDB wird auch von anderen Remote-CA ITCM-Managern verwendet, z. B.:
		`11:36:50 ** Active DB Processes **`
		`11:36:50 DB Processes for`
		`11:36:50 DB Name = mdb, Node = UNI6505L3-065, Process = CA IT Client Manager r12`
		`11:36:50 DB Name = mdb, Node = CMQA158, Process = CA IT Client Manager r12`
		`11:36:50 DB Processes for`
		`11:36:50 ** End DB Processes **`
		`11:36:50 There are active processes connected …`
		Dieser Fall ist in der Praxis unwahrscheinlich und tritt nur dann ein, wenn das gesamte CA ITCM-System falsch konfiguriert ist oder in der falschen Reihenfolge konfiguriert wird.
		Beenden Sie die Remote-Prozesse vorübergehend. Die Protokolldatei gibt an, welche Remote-Hosts betroffen sind.

Fehlertext (in %TEMP%\ TRC_Inst2_ITRM.log)	**Bedingungen**	**Diagnosen und Maßnahmen**
Der MSSQL-Server wird nicht auf \\local_host ausgeführt.	Die MDB ist remote; lokale und Remote-Hosts befinden sich nicht in derselben Domäne.	Diese Meldung ist irreführend, da kein Kontakt zum Remote-MDB-Host hergestellt wird. Fügen Sie den lokalen Host zur selben Domäne hinzu wie den Remote-Host.

A Dependency checker test has failed.	Terminaldienste sind auf dem Host aktiviert.	Deaktivieren Sie während der CCS-Installation vorübergehend die Terminaldienste. Eine Installation auf der Konsole bietet sich u. U. ebenfalls an.
		Oder wie es im *CCS/NSM-Implementierungshandbuch* (nur auf Englisch verfügbar) heißt: "… in diesem Release werden Installationen über Windows-Terminaldienste sogar bei einer Konfiguration im Anwendungsservermodus unterstützt." Jedoch sind die folgenden Einstellungen erforderlich:
		■ Der CONSOLE-Modus muss bei Installationen über Remote-Zugriff verwendet werden.
		Beispiel:
		`mstsc /v:HostName /console`
		■ Vor der Installation sollten die USER-Einstellungen für den Terminal-Server in INSTALL geändert werden.
		Beispiel:
		`change user /install`
		Um die Benutzereinstellungen zu überprüfen, führen Sie den folgenden Befehl aus:
		`change user /query`
		Weitere Informationen zum Hilfsprogramm CHANGE USER der Windows-Terminaldienste finden Sie unter http://support.microsoft.com/kb/186504 http://support.microsoft.com/kb/186504.

Vorbedingungen für die DSM-Manager-Installation

Unter Umständen sind andere CA Technologies-Produkte auf dem DSM-Managersystem installiert, auf dem bereits eine MDB installiert ist.

Stellen Sie sicher, dass kein anderes Produkt die MDB verwendet, bevor Sie die Installation eines DSM-Managers starten. Wenn ein anderes Produkt die MDB verwendet, reagiert der Installationsprozess u. U. nicht mehr.

Wenn Sie CA ITCM unter Windows nach Unicenter Asset Portfolio Management installieren möchten, prüfen Sie zunächst, ob der Prozess "corasmm.exe" ausgeführt wird. In diesem Fall stellen Sie den Unicenter Asset Portfolio Management-Benachrichtigungsserver und den Unicenter Asset Portfolio Management-Zwischenspeicherdienst auf manuellen Modus ein und starten den Computer erneut, bevor Sie CA ITCM installieren. Wenn die Installation von CA ITCM abgeschlossen ist, müssen Sie die beiden Unicenter Asset Portfolio Management-Dienste erneut starten und aktivieren. Dies kann über den Dienststeuerungs-Manager unter "Systemsteuerung", "Verwaltung", "Dienste" erfolgen.

Hinweise zur Festplattenkapazität bei der Installation des DSM-Managers und der MDB

Installieren Sie den DSM-Manager auf einer Partition mit mindestens 12 GB freiem Speicherplatz. Die Installation selbst beansprucht ca. 7,7 GB auf der Festplatte und benötigt gelegentlich mehr Platz für die Protokolldateien. Wenn auch die MDB-Datenbank auf dieser Partition installiert wird, müssen Sie mindestens 50 GB zusätzlich für die Datenbank (sowohl SQL Server als auch Oracle) und den damit verknüpften Online-Checkpoint sowie die Journaldateien einplanen. Eine umfangreiche SQL Server- oder Oracle-Datenbank kann bis zu 100 GB beanspruchen. Diese Angaben sind unabhängig von Ihren Anforderungen an die Datenspeicherung für zu verteilende Softwarepakete. Weitere Informationen finden Sie im Kapitel "Hardwarespezifikationen und -anforderungen" in den *Versionshinweisen zu CA IT Client Manager*, die in der CA IT Client Manager-Dokumentation (Bookshelf) enthalten sind.

Ein Neustart ist nach der Installation normalerweise nicht erforderlich, kann aber die Leistung steigern, da mehr Systemressourcen verfügbar werden.

Für die Datenreplikation zwischen Domäne und Enterprise muss die tempdb-Datenbank eine bestimmte Mindestgröße aufweisen. Daher muss den tempdb-Dateien und dem Transaktionsprotokoll unbedingt genügend Speicher zugeordnet werden. Es wird empfohlen, als anfängliche Dateigröße für die tempdb-Datenbank auf der Domänenebene 80 MB und auf der Enterprise-Ebene 2 GB festzulegen. Darüber hinaus müssen Sie sicherstellen, dass die autogrowth-Eigenschaft auf "unrestricted growth" eingestellt ist.

Eigenständiger Manager in einer gemischten Datenbankumgebung

Wenn Sie einen eigenständigen Domänen-Manager installieren und ihn anschließend mit einem Enterprise-Manager verknüpfen möchten, der einen anderen MDB-Datenbanktyp verwendet, müssen Sie den entsprechenden Datenbank-Client manuell auf dem Domänen-Manager installieren. Dann kann der Domänen-Manager eine Verbindung zum Enterprise-Manager zur Replikation herstellen.

Wenn der Domänen-Manager z. B. Microsoft SQL Server und der Enterprise-Manager Oracle verwendet, müssen Sie auf dem Domänen-Mananger den Oracle-Datenbank-Client installieren.

Unbeaufsichtigte MDB-Installation mithilfe einer Antwortdatei

Das MDB-Installationsprogramm unterstützt die unbeaufsichtigte Installation von einer Antwortdatei mithilfe des Befehls "setup.bat -r response_file" unter Windows bzw. "setup.sh -r response_file" unter Linux/Solaris.

Das MDB-Installationsprogramm unterstützt auch die Erstellung einer Antwortdatei mithilfe des Befehls "setup.bat -g-response_file" unter Windows bzw. "setup.sh -g response_file" unter Linux/Solaris.

Anstelle eine Antwortdatei zu generieren, können Sie die Antwortdateivorlage "install.rsp" bearbeiten und diese Vorlage verwenden, um eine unbeaufsichtigte Installation durchzuführen.

Verschlüsselung und Entschlüsselung von Kennwörtern in einer Antwortdatei

Standardmäßig verwenden MDB-Installationsprogramme das Blowfish-Verschlüsselungs- und Entschlüsselungshilfsprogramm, das in den MDB-Paketen enthalten ist: "blfs.exe" unter Windows und "blfs" unter Linux und Solaris. Wenn Sie Setup mit der Option "-g" ausführen, verwendet die Anwendung automatisch Blowfish, um Kennwörter in der Antwortdatei zu verschlüsseln.

Wenn Sie die Antwortdatei erstellen, indem Sie die enthaltene Vorlage "install.rsp" bearbeiten, führen Sie das Blowfish-Hilfsprogramm über einen Befehl oder ein Shell-Fenster aus, um das Kennwort zu verschlüsseln. Kopieren Sie dann die sich ergebende Zeichenfolge in die Antwortdatei.

Wenn beispielsweise der Befehl "blfs validation_0101" auf Linux/Solaris die verschlüsselte Zeichenfolge "0x530924b11654032a6e0e213281cd8565c3f9ec63b09dc673" zurückgibt, müssen Sie diese Zeichenfolge wie folgt in die Antwortdatei kopieren:

```
# Password of Oracle MDB admin user
ITRM_MDBADMINPWD=0x530924b11654032a6e0e213281cd8565c3f9ec63b09dc673
```

In beiden Fällen: Wenn Sie Setup mit der Option "-r" ausführen, verwendet die Anwendung automatisch das Blowfish-Hilfsprogramm, um Kennwörter in der Antwortdatei zu verschlüsseln.

Hinweis: Die unverschlüsselten Kennwörter dürfen nicht mit "0x" beginnen (Groß- und Kleinschreibung muss beachtet werden).

Der Blowfish-Algorithmus ist nicht FIPS-kompatibel. Sie können ein benutzerdefiniertes FIPS-kompatibles Hilfsprogramm für Verschlüsselung oder Entschlüsselung angeben, indem Sie Umgebungsvariablen festlegen, die auf die entsprechenden Programme zeigen. Legen Sie demnach "MDB_ENC_PROG" auf den vollständigen Pfadnamen des Verschlüsselungsprogramms und "MDB_DEC_PROG" auf den vollständigen Pfadnamen des Entschlüsselungsprogramms fest.

Beispiel: Ändern von Verschlüsselungs- oder Entschlüsselungsprogrammen unter Windows

```
set MDB_ENC_PROG=E:\tmp\my_encrypter.exe

set MDB_DEC_PROG=E:\tmp\my_decrypter.exe
```

Unter Windows müssen die Programme eine EXE-Erweiterung im Dateinamen aufweisen.

Beispiel: Ändern von Verschlüsselungs- oder Entschlüsselungsprogrammen unter Solaris oder Linux

```
MDB_ENC_PROG=/tmp/my_encrypter
export MDB_ENC_PROG

MDB_DEC_PROG=/tmp/my_decrypter
export MDB_DEC_PROG
```

Wenn Sie "MDB_DEC_PROG" nicht festlegen oder wenn das Programm nicht vorhanden ist, wird angenommen, dass "MDB_DEC_PROG" "MDB_ENC_PROG" entspricht. Wenn Sie "MDB_ENC_PROG" nicht festlegen oder wenn das Programm nicht vorhanden ist, werden die standardmäßigen Blowfish-Verschlüsselungs- und Entschlüsselungsprogramme verwendet.

Vorbereitung für das Arbeiten mit einer Microsoft SQL Server-MDB

Bevor Sie einen DSM-Manager auf Grundlage von Microsoft SQL Server installieren, muss SQL Server mit der folgenden Konfiguration installiert worden sein:

- Authentifizierung im gemischten Modus (d. h. Windows-Authentifizierung und SQL Server-Authentifizierung) erforderlich.
- Das TCP/IP-Netzwerkprotokoll ist aktiviert und betriebsbereit. Informationen zur Auswahl und Konfiguration von Netzwerkprotokollen finden Sie in der Dokumentation zu SQL Server.
- Die folgende Regel gilt für die Server-Sortierreihenfolge, die während der Installation von SQL Server ausgewählt wurde:

  Sie müssen einen Sortierungsnamen wählen, bei dem eine Variante ohne Beachtung der Groß-/Kleinschreibung unterstützt wird.

Verwenden Sie den CA ITCM-Installationsassistenten und befolgen Sie die Anweisungen zum Konfigurieren der SQL Server-MDB, wie hier beschrieben:

- Auf der Assistentenseite "Manager konfigurieren" müssen Sie die obligatorischen Spezifikationen (Verbindungsparameter) für das Zieldatenbanksystem eingeben, z. B.:
  - Management-Datenbankprovider (wählen Sie "Microsoft SQL Server")
  - Management-Datenbankserver
  - MDB-Kennwort

    Hinweis: Da die Authentifizierung im gemischten Modus verwendet wird, muss dieses Kennwort der Sicherheitsebene eines Systemanmeldungskennworts entsprechen.
- Auf der Seite "Microsoft SQL Server-MDB konfigurieren" können Sie die folgenden Konfigurationseinstellungen eingeben:
  - Kompatibilitätsmodus

    Hinweis: Das Kontrollkästchen für den Kompatibilitätsmodus muss ausgewählt sein, wenn Sie eine neue MDB 1.5 wie mit dem Produkt ausgeliefert installieren möchten und Sie vorhaben, später ein weiteres CA Technologies-Produkt zu installieren, das nur MDB 1.0.4 unterstützt. Wenn das Kontrollkästchen für den Kompatibilitätsmodus nicht ausgewählt ist, schlägt die Installation aller Folgeprodukte, die MDB 1.5 nicht unterstützen, fehl.

    Standard: Der Kompatibilitätsmodus ist nicht ausgewählt.
  - MDB-Datenbankname

    Standard: MDB
  - MDB-Instanzname

    Wählen Sie den Instanznamen in der Dropdown-Liste aus.

Standard: default

- Datenbank-Portnummer

  Standard: 1433

Während der Installation müssen Sie für alle nicht standardmäßigen Instanzen die Port-Nummer eingeben, die der Microsoft SQL Server-Instanz zugeordnet ist. Der Port kann mit SQL Server Configuration Management in der SQL Server-TCP/IP-Konfiguration nachgeschlagen werden.

Wenn Microsoft SQL Server mit benannten Instanzen konfiguriert wird, wird für die Option "Dynamische TCP-Ports" automatisch die Port-Nummer angegeben (dynamische Port-Konfiguration). Manchmal kann der Domänen- oder Enterprise-Manager dann nicht auf die Datenbank zugreifen, da die Port-Nummer auf dem MDB-System in der Zwischenzeit geändert wurde, beispielsweise aufgrund eines Systemneustarts. Um derartige Zugriffsfehler zu vermeiden, wird empfohlen, die Port-Einstellung manuell in eine statische Port-ID zu ändern, wie nachfolgend beschrieben:

- Öffnen Sie im Windows-Startmenü SQL Server Konfigurations-Manager, SQL Server Netzwerkkonfiguration, Protokolle für *instance_name*, TCP/IP.
- Klicken Sie mit der rechten Maustaste darauf, und wählen Sie im Kontextmenü die Option "Eigenschaften".
- Wählen Sie im Dialogfeld für TCP/IP-Eigenschaften die Registerkarte "IP-Adressen" aus. Kopieren Sie den Port-Wert im Bereich "IPAll" aus dem Feld "Dynamische TCP-Ports" in das Feld "TCP-Port".

Wichtig! Wenn Sie eine nicht standardmäßige Port-Nummer manuell zuweisen, wird empfohlen, dass Sie die Liste "reservedPorts" in der Registrierung aktualisieren. Anderenfalls könnte, wenn CAF nach einem Neustart vor SQL Server gestartet wird und eine dynamische Port-Nummer anfordert, CAF die Port-Nummer erhalten, die für SQL Server festgelegt wurde. Dies führt dazu, dass SQL Server beim Start fehlschlägt.

Installieren des DSM-Managers: Microsoft SQL Server-MDB

Nachdem Sie die Installation der Microsoft SQL Server-MDB fertig gestellt haben, installieren Sie den DSM-, Enterprise- oder Domänen-Manager.

Gehen Sie folgendermaßen vor:

1. Installieren Sie den Microsoft-SQL-Client auf dem Computer, auf dem Sie Ihren DSM-, Enterprise- oder Domänen-Manager installieren möchten.

   Hinweis: Dieser Schritt ist nicht notwendig, wenn Microsoft SQL Server bereits auf dem Computer installiert ist.

2. Installieren Sie den CA ITCM-DSM-Manager, und geben Sie die Informationen Ihrer Microsoft SQL Server-MDB in den relevanten Dialogfeldern ein.
3. Starten Sie CAF.

Remote-MDB-Installation für Microsoft SQL Server

Wenn Sie den DSM-Manager über eine Microsoft SQL Server-basierte Remote-MDB ausführen möchten, müssen der Manager-Computer und der Remote-MDB-Computer in einem Vertrauensverhältnis zueinander stehen, wenn sie in einer Windows-Umgebung ausgeführt werden.

Während der Installation eines Domänen- oder Enterprise-Managers können Sie die MDB auf dem lokalen Host installieren oder eine bestehende Remote-Instanz der MDB verwenden.

Installieren Sie für eine Remote-Konfiguration die Datenbank auf dem Remote-Computer durch Auswahl von "MDB installieren" (keine CCE-Funktionalität).

Wenn Sie CCE mit CA ITCM verwenden müssen, müssen Sie CCE auf dem MDB-Hostcomputer installieren, und zwar entweder lokal oder remote. Verwenden Sie die Option "CCS installieren" im CA ITCM-Installationsdialogfeld auf oberster Ebene. Installieren Sie dann den Domänen- oder Enterprise-Manager.

Wenn Sie einen Remote-Microsoft-SQL Server verwenden, installieren Sie die Microsoft SQL-Client-Verwaltungstools, *bevor* Sie den Domänen- oder Enterprise-Manager installieren. Stellen Sie sicher, dass die Auswahl der Microsoft SQL-Client-Verwaltungstools während der Installation des Microsoft SQL-Clients nicht aufgehoben ist.
CA ITCM verwendet den spezifischen, auf Datenbankebene erstellten Benutzer "ca_itrm", um sich für den MDB-Zugriff zu authentifizieren. Das gleiche Kennwort für den Benutzer "ca_itrm" muss in "MDB installieren" und den Dialogfeldern der CA ITCM-Installation angegeben werden. Der Benutzer "ca_itrm" wird automatisch erstellt.
Wenn Sie mehrere Domänen-Manager mit entfernten Microsoft SQL Server-MDBs installieren, darf nur eine MDB auf jeder Datenbankserverinstanz vorhanden sein. Sie müssen demnach über genauso viele Datenbankserver wie MDBs verfügen.

Hinweis: Bei Verwendung einer entfernten Microsoft SQL Server-MDB wird der Name des die Domänen-MDB hostenden Servers als Domänen-Manager-Name verwendet. Daher zeigt der DSM-Explorer im Enterprise-Manager den Domänen-Manager mit dem Namen seines Datenbankservers an.

Vorbereitung für das Arbeiten mit einer Oracle-MDB

Verwenden Sie den CA ITCM-Installationsassistenten, um den Manager für das Arbeiten mit einer Oracle-MDB zu konfigurieren, wie nachfolgend beschrieben. Es ist wichtig, dass die in diesen Konfigurationsschritten angegebenen Parameterwerte mit den während der Oracle MDB-Installation angegebenen Parameterwerten übereinstimmen:

- Auf der Assistentenseite "Manager konfigurieren" müssen Sie die obligatorischen Spezifikationen (Verbindungsparameter) für das Zieldatenbanksystem eingeben, z. B.:
  - MDB-Provider (wählen Sie "Oracle")
  - MDB Server
  - MDB-Kennwort
  - Datenbankadministrator (sys)

    (Weitere Informationen finden Sie unter Datenbankadministrator-Benutzer auf Oracle (siehe Seite 130).)
  - Datenbankadministratorkennwort
- Klicken Sie im Bereich "Erweiterte Manager-Konfiguration" auf die Schaltfläche "Datenbank", um eine weitere Assistentenseite zu öffnen, auf der Sie erweiterte Konfigurationseinstellungen für eine benutzerdefinierte MDB-Installation angeben können.
- Auf der Seite "Oracle-MDB konfigurieren" können Sie erweiterte Konfigurationseinstellungen eingeben, z. B.:
  - Kompatibilitätsmodus

    Hinweis: Das Kontrollkästchen für den Kompatibilitätsmodus muss ausgewählt sein, wenn Sie eine neue MDB 1.5 wie mit dem Produkt ausgeliefert installieren möchten und Sie vorhaben, später ein weiteres CA Technologies-Produkt zu installieren, das nur MDB 1.0.4 unterstützt. Wenn das Kontrollkästchen für den Kompatibilitätsmodus nicht ausgewählt ist, schlägt die Installation aller Folgeprodukte, die MDB 1.5 nicht unterstützen, fehl.

    Standard: Der Kompatibilitätsmodus ist nicht ausgewählt.
  - MDB-Datenbankname

    Standard: orcl
  - Datenbank-Portnummer

    Standard: 1521
  - MDB-Administratorkennwort

Voraussetzungen

In diesem Abschnitt werden die Voraussetzungen für die Installation der MDB auf Oracle 11g aufgelistet:

- Installieren Sie den Oracle 11g-Server auf dem Computer, auf dem Sie die MDB entweder installieren oder aktualisieren werden. Diese Version unterstützt Windows-, Solaris- und Linux-Server für Oracle 11g-MDBs.
- Erstellen Sie eine Oracle-Instanz mithilfe des Assistenten für die Oracle-Datenbankkonfiguration. Berücksichtigen Sie die folgenden Faktoren, während Sie die Instanz erstellen:
  - Der Datenbankinstanzname (SID) muss dem Namen des Oracle-Dienstes (globaler Name) entsprechen.
  - Entsprechende Werte müssen in die Felder für die SGA- und PGA-Größe auf der Registerkarte "Arbeitsspeicher" im Assistenten für die Oracle-Datenbankkonfiguration eingegeben werden.

    Ein Minimum von 2 GB wird für SGA empfohlen.
- Installieren den Sie Oracle 11g-Client auf dem Computer, auf dem Sie den CA ITCM DSM-Manager installieren oder aktualisieren werden.

Hinweis: Ausführliche Installationsanweisungen finden Sie im entsprechenden Installationshandbuch, das in der Oracle-Dokumentationsbibliothek verfügbar ist.

Datenbankadministrator-Benutzer auf Oracle

Für die Installation des Managers wird ein Oracle-Administrator-Benutzer benötigt. Wenn Sie den Oracle-Benutzer "SYS" verwenden möchten, stellt der Installer die Verbindung mit "as sysdba" her. Sie können jedoch auch einen anderen Benutzer verwenden. In diesem Fall muss der Benutzer als ein Benutzer erstellt werden, der dieselben Berechtigungen besitzt wie SYSDBA. Dies bedeutet, dass diesem Benutzer die SYSDBA-Berechtigungen gewährt werden.

Für die folgenden Vorgänge auf Oracle muss der Benutzer SYSDBA-Berechtigungen besitzen, um sie ausführen zu können:

- Starten einer Datenbank
- Beenden einer Datenbank
- Sichern einer Datenbank
- Wiederherstellen einer Datenbank
- Erstellen einer Datenbank

Installieren einer Oracle-MDB (eigenständig)

Wichtig! Notieren Sie sich die Werte und Kennwörter, die Sie in den Schritten im Installationsassistenten eingeben, da Sie diese später für die Konfiguration des DSM-Managers benötigen.

Die grundlegenden Schritte für die Installation der MDB auf Oracle 11 g im interaktiven Modus lauten:

1. Erstellen Sie eine Oracle-Instanz mithilfe des Assistenten für die Oracle-Datenbankkonfiguration (sofern noch nicht geschehen), und führen Sie folgende Aktionen aus:
   - Stellen Sie sicher, dass der Datenbankinstanzname (SID) dem Namen des Oracle-Dienstes (globaler Name) entspricht.
   - Geben Sie die entsprechenden Werte in die Felder für die SGA- und PGA-Größe auf der Registerkarte "Arbeitsspeicher" im Assistenten für die Oracle-Datenbankkonfiguration ein.
2. Führen Sie die entsprechende Skriptdatei auf dem Zieldatenbankserver vom MDB-Verzeichnis aus:

   Gültig für Windows

   ```
   setup.bat
   ```

   Gilt für Solaris und Linux

   ```
   sh ./setup.sh
   ```

   Das MDB-Installationsprogramm wird gestartet, und die erste Seite des Assistenten "Setup-Sprache auswählen" wird angezeigt.
3. Akzeptieren Sie Englisch als Setup-Sprache.

   Hinweis: Diese Version ist nur in englischer Sprache verfügbar.
4. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung.
5. (nur Windows) Wählen Sie den Datenbanktyp, Oracle-Server für diese Prozedur aus.
6. Geben Sie den Pfad der Oracle-Installation für die MDB im Feld "ORACLE_HOME" ein, um die funktionierende Laufzeit-Oracle-Umgebung zu definieren.

   Geben Sie für die Remote-MDB-Installation den Wert "ORACLE_HOME" Ihres lokalen Computers ein.
7. Geben Sie den Oracle-Datenbankservernamen und die MDB-Größe an.
8. Geben Sie die MDB-Benutzer und -Datenbank-Administratoranmeldeinformationen an.

   Hinweis: Der Standard-MDB-Benutzername ist "ca_itrm".

9. Geben Sie erweiterte Oracle-Konfigurationseinstellungen ein. Dazu zählen der Name des Oracle-Dienstes, der Oracle-TNS-Name (Oracle Transparent Network Substrate), die Portnummer, der Tablespace-Pfad und das MDB-Administratorkennwort.
10. Überprüfen Sie Ihre Datenbankkonfigurationsoptionen, und bestätigen Sie die Installation, indem Sie auf die Schaltfläche "Installieren" klicken.

    Die Installation wird gestartet, und das MDB-Schema wird in der Oracle-Datenbank erstellt.

    Hinweis: Im MDB-Installationsprogramm unter Solaris wird ein Dialogfeld angezeigt, in dem die Oracle-Version und die Betriebssystem-Voraussetzungsprüfungen angegeben sind. Beim neuen MDB-Installationsprogramm wird dieses Dialogfeld nur angezeigt, wenn bei den Voraussetzungen Fehler vorliegen, andernfalls wird die Installation einfach fortgesetzt.
11. Installieren Sie den DSM-Manager, wenn die Installation der Oracle-MDB abgeschlossen ist.

Hinweis: Der DSM-Manager verwendet EZCONNECT, um eine Verbindung zur Oracle-MDB herzustellen.

Weitere Informationen:

Remote-MDB-Installation für Oracle (siehe Seite 136)
Installieren des DSM-Managers: Oracle-MDB (siehe Seite 133)
Unbeaufsichtigte MDB-Installation mithilfe einer Antwortdatei (siehe Seite 124)

Installieren des DSM-Managers: Oracle-MDB

Installieren Sie DSM-, Enterprise- oder Domänen-Manager.

Gehen Sie folgendermaßen vor:

1. Installieren Sie den Oracle 11g-Client auf dem Computer, auf dem Sie Ihren DSM-, Enterprise- oder Domänen-Manager installieren möchten.
2. Installieren Sie den CA ITCM-DSM-Manager, und geben Sie die Informationen Ihrer Oracle-MDB in den relevanten Dialogfeldern ein.

   Hinweis: Wenn für die Installation des Managers der Name des MDB-Oracle-Server erforderlich ist, geben Sie die IP-Adresse nur dann ein, wenn sich der Manager und die MDB auf demselben Computer befinden. Geben Sie ansonsten den Host- oder DNS-Namen ein.
3. Folgen Sie den Anweisungen des Assistenten, um die Installation des Managers abzuschließen.
4. Führen Sie die folgenden zusätzlichen Schritte aus, wenn der DSM-Manager auf dem gleichen Computer wie die Windows-Oracle-MDB installiert wird:
   a. Führen Sie den folgenden SQL-Befehl als "mdbadmin" aus:

      ```
      update ca_n_tier set
              label='<MDB Server host name>',
              db_host_name='<MDB Server host name>',
              db_server='<MDB Server DNS name>'
      wobei "domain_uuid in (select set_val_uuid from ca_settings where
      set_id=1)"
      ```

   b. Überprüfen Sie, ob die Aktualisierung ausgeführt wird. Wenn der automatische Commit deaktiviert ist, führen Sie ein manuelles Update durch.

   c. Führen Sie folgenden Befehl an der Eingabeaufforderung aus:

      ```
      ccnfcmda -cmd setparametervalue -ps /itrm/database/default -pn dbmsserver
      -v <MDB Server DNS name>
      ```
5. Starten Sie CAF.

Weitere Informationen:

Installieren einer Oracle-MDB (eigenständig) (siehe Seite 131)

Installation einer Remote-Oracle-MDB

Zum Installieren einer Remote-Oracle-MDB müssen Sie zunächst auf einem Remote-Computer mit einem Sun Solaris-Betriebssystem mit Hilfe des Assistenten für die Oracle-Datenbankkonfiguration eine Oracle-Instanz erstellen.

So installieren Sie die Oracle-MDB:

1. Melden Sie sich beim Solaris-Host als Benutzer "root" an und navigieren Sie zu *DVD-Mount*/SolarisProductFiles_MDB/remotemdb.
2. Führen Sie "sh ./setup.sh" aus.
3. Wählen Sie die Option "Setup-Sprache für Installation wählen".

   Die für den Installationsassistenten verfügbaren Sprachen sind Englisch, Französisch, Deutsch und Japanisch.
4. Wählen Sie "Neue Instanz" und befolgen Sie die Anweisungen des Assistenten.

   Wichtig! Notieren Sie sich die Werte und Kennwörter, die Sie in den folgenden Schritten eingeben, da Sie diese später für die Konfiguration des DSM-Managers benötigen.
5. Sie müssen die Endbenutzer-Lizenzvereinbarung lesen und akzeptieren, bevor der Installationsassistent fortfährt.
6. Geben Sie für die Umgebungsvariable ORACLE_HOME den Pfad der Oracle-Installation an, den Sie für die MDB verwenden möchten.

   Das Installationsprogramm überprüft die Hardware-Plattform und die ORACLE-Umgebung. Bei einem negativen Testergebnis wird die Installation nicht durchgeführt. Nur wenn alle Tests erfolgreich sind, kann der Benutzer im Installationsassistenten fortfahren.
7. Wählen Sie einen Produktinstanznamen für die aktuelle Installation. Dieser entspricht in der Regel dem Namen der ORACLE-Instanz (SID).

   In der Dropdown-Liste "Auswahl des Produktnamens" werden Namen angezeigt, die bereits verwendet werden. Der Name der Produktinstanz muss eindeutig sein.
8. Geben Sie das Kennwort für den MDB-Benutzernamen (ca_itrm) ein.

   Das Kennwort wird während der Installation festgelegt, und es wird eine Bestätigung angefordert. Merken Sie sich das Kennwort.
9. Geben Sie den DB-Administratornamen (Standardname "sys") und das DB-Administratorkennwort ein. Der DB-Administrator ist ein *Benutzername*, dem in der Oracle-Instanz die SYSDBA-Berechtigung erteilt wurde.

   Hinweis: Weitere Informationen finden Sie in der *MDB-Übersicht*, die in der CA ITCM-Dokumentation (Bookshelf) enthalten ist.

10. Geben Sie an, ob der Kompatibilitätsmodus installiert werden soll.

    Hinweis: Das Kontrollkästchen für den Kompatibilitätsmodus muss ausgewählt sein, wenn Sie eine neue MDB 1.5 wie mit dem Produkt ausgeliefert installieren möchten und Sie vorhaben, später ein weiteres CA Technologies-Produkt zu installieren, das nur MDB 1.0.4 unterstützt. Wenn das Kontrollkästchen für den Kompatibilitätsmodus nicht ausgewählt ist, schlägt die Installation aller Folgeprodukte, die MDB 1.5 nicht unterstützen, fehl.

    Standard: Der Kompatibilitätsmodus ist nicht ausgewählt.

11. Geben Sie im Feld "MDB-Datenbank" die SID der Oracle-Datenbankinstanz an, die Sie für die MDB verwenden möchten.

    Der Wert dieses Felds ist standardmäßig der auf der vorherigen Assistentenseite eingegebene Produktinstanzname.

12. Geben Sie die Datenbank-Portnummer an.

    Standard: 1521

    Wichtig! Die Portnummer, die Sie hier eingeben, hängt von der bei der Datenbankerstellung verwendeten Portnummer ab. Wurde zum Zeitpunkt der Datenbankerstellung eine nicht standardmäßige Portnummer verwendet, muss dieselbe Portnummer beim Installieren der MDB eingegeben werden. Ändern Sie andernfalls nicht die standardmäßige Datenbank-Portnummer.

13. Geben Sie den Tablespace-Pfad an, d. h. das Verzeichnis, in dem Oracle die Datenbankdateien erstellt. Alle Verzeichnisse in diesem Pfad müssen bereits vorhanden sein, mit Ausnahme des letzten Verzeichnisses. Beispielsweise muss bei dem Standardpfad, der im Assistenten voreingestellt ist, das Verzeichnis "mdb" noch nicht existieren.

    Standard: /opt/CA/SharedComponents/oracle/mdb

14. Im Feld "MDB-Administratorkennwort" müssen Sie das Kennwort des MDBADMIN-Benutzers angeben.

    Der Datenbankbenutzer MDBADMIN wird für die Erstellung des MDB-Schemas verwendet und ist der Eigentümer des Schemas.

15. Bei dem Schritt "MDB installieren" im Assistentenprozess müssen Sie die Installation bestätigen, indem Sie auf die Schaltfläche "Installieren" klicken.

    Erst nach dieser Bestätigung wird das MDB-Schema in der Oracle-Datenbank erstellt.

Wichtig! Wenn Sie eine Remote-Oracle-MDB verwenden, muss auf dem Manager und auf jedem System, auf dem eine DSM-Engine oder der DSM-Reporter ausgeführt wird, ein Oracle 11*g*-Client verfügbar sein. Stellen Sie sicher, dass der Oracle 11*g*-Client vom Typ "Administrator" installiert ist.

Weitere Informationen:

Oracle-MDB-Wartung (siehe Seite 214)

Remote-MDB-Installation für Oracle

Hinweis: Die Remote-MDB-Installation auf einer Oracle-Datenbank wird nur von Windows unterstützt.

Für eine Remote-Installation verweist die Umgebungsvariable ORACLE_HOME auf den lokalen Computer (auf dem Sie möglicherweise nur über einen Oracle-Client verfügen).

Definieren Sie für Installationen und Upgrades für eine Oracle-MDB einen TNS-Namen für den Remote-Computer in der Oracle-Datei "tnsnames.ora" des lokalen Computers. Mithilfe dieser Aktion kann der Remote-Oracle-Server adressiert werden.

Bei einer lokalen Oracle-MDB-Installation erstellt das MDB-Installationsprogramm den angegebenen Tablespace-Ordnerpfad, sofern er nicht vorhanden ist. Dieser Schritt ist bei einer Remote-Installation nicht möglich. Überprüfen Sie daher, ob der Tablespace-Ordnerpfad, den Sie während der MDB-Installation auswählen werden, auf dem Remote-Computer vorhanden ist. Wenn der Tablespace-Ordner auf dem Remote-Computer nicht vorhanden ist, tritt ein Fehler auf, und die Installation wird nicht weiter fortgesetzt.

Weitere Informationen:

Installieren einer Oracle-MDB (eigenständig) (siehe Seite 131)

Hinweis zu CCS-Unterstützung für Oracle

CA Common Services (CCS) unterstützt derzeit keine Oracle-MDB.

Deshalb steht in CA ITCM eine Teilmenge von CCS mit eingeschränktem Funktionsumfang zur Verfügung, die vorrangig auf die Anforderungen von CA ITCM abgestimmt ist, hauptsächlich auf die Unterstützung für Ereignisse (Kalender) und IPv6.

Der Installer wählt automatisch die geeignete Version von CCS für Ihre Umgebung aus.

Hinweise zur Installation und Konfiguration für die Oracle-MDB

Der folgende Abschnitt enthält Hinweise zur Installation und Konfiguration der Oracle-MDB.

Installation des Solaris Oracle-Servers

Ausführliche Installationsanweisungen finden Sie im Installationshandbuch, das in der Oracle-Dokumentationsbibliothek verfügbar ist.

Löschen und erneutes Erstellen einer Oracle-Datenbankinstanz

Verwenden Sie den Assistenten für die Oracle-Datenbankkonfiguration zum Löschen und Erstellen einer Oracle-Datenbankinstanz. Während der Erstellung einer Oracle-Datenbankinstanz mit Hilfe dieses Tools werden sie aufgefordert, die Arbeitsspeichergröße anzugeben, die Oracle für diese Instanz verwenden kann. Geben Sie entsprechende Werte in die Felder für die SGA- und PGA-Größe in der Registerkarte "Arbeitsspeicher" ein.

Geben Sie beispielsweise "1198" in das Feld für die SGA-Größe und "399" in das Feld für die PGA-Größe ein. Diese empfohlenen Werte entsprechen ungefähr 1,2 GB für die Daten- und Steuerinformationen (SGA) und ungefähr 0,4 GB für den Programmbereich (PGA). Dies sind die empfohlenen Mindestwerte für eine Installation mit bis zu 10.000 Computer-Assets.

Überprüfen der Oracle-Serverinstallation

Sie müssen die richtige Oracle-Version und Patch-Ebene installiert haben. Andernfalls schlagen Operationen des DSM-Managers möglicherweise fehl. Führen Sie zur Überprüfung der Oracle-Version und Patch-Ebene den folgenden Befehl aus:

```
goto $ORACLE_HOME/OPatch
call ./opatch lsinventory
```

Konfiguration der Oracle-MDB zur Unterstützung von Multibyte-Sprachen

Wählen Sie bei der Erstellung einer Oracle-Datenbankinstanz mit Hilfe des Assistenten für die Oracle-Datenbankkonfiguration die Option "Use Unicode (AL32UTF8)" in der Registerkarte "Zeichensätze", um Multibyte-Sprachen zu unterstützen.

Ändern des Standardkennwortes für den Benutzer "ca_itrm".

Während der Installation des Managers oder der MDB können Sie das Kennwort für den Benutzer "ca_itrm" ändern, das für den MDB-Zugriff verwendet wird.

Zum Ändern des Kennwortes für den Benutzer "ca_itrm" müssen Sie einige Schritte ausführen, die vom Datenbankprovider abhängig sind:

- Microsoft SQL Server-MDB
- Oracle-MDB

Ändern des Standardkennworts bei Verwendung von Microsoft SQL Server

Wenn Sie das Standard-Kennwort für den Benutzer "ca_itrm" ändern möchten, wenn Microsoft SQL Server als Datenbank-Provider verwendet wird, gehen Sie wie folgt vor:

1. Wechseln Sie zu dem System, auf dem Microsoft SQL Server ausgeführt wird.
2. Wählen Sie im Windows-Startmenü "Programme", "Microsoft SQL Server Management Studio".
3. Wählen Sie den Benutzer "ca_itrm" in Management Studio und ändern Sie das Kennwort.
4. Wechseln Sie zu dem System, auf dem der Manager installiert wurde.
5. Führen Sie "cadsmcmd setDBCredentials passwd=*neues_Kennwort*" aus.
6. Führen Sie "caf stop" aus.
7. Führen Sie "caf start" aus.

Ändern des Standardkennworts bei Verwendung von Oracle

Wenn Sie das Standard-Kennwort für den Benutzer "ca_itrm" ändern möchten, wenn Oracle als Datenbank-Provider verwendet wird, gehen Sie wie folgt vor:

1. Wechseln Sie zu dem System, auf dem Oracle ausgeführt wird.
2. Wählen Sie im Windows-Startmenü "Programme" und starten Sie die entsprechende Oracle Database Control.
3. Wählen Sie den Benutzer "ca_itrm" in der Oracle Database Control und ändern Sie das Kennwort.
4. Wechseln Sie zu dem System, auf dem der Manager installiert wurde.
5. Führen Sie "cadsmcmd setDBCredentials passwd=*neues_Kennwort*" aus.
6. Führen Sie "caf stop" aus.
7. Führen Sie "caf start" aus.

Protokolldateien zur MDB-Installation

Wenn eine Microsoft SQL Server-MDB auf einem Windows-Computer installiert wird, befinden sich die Protokolldateien an den folgenden Speicherorten:

- %TEMP%\ITRM\database\setup.log
- %TEMP%\ITRM\database\mdb_install\install_*xxxx*.log
- *CA ITCM-Installationsverzeichnis*\database\setup.log

Wenn eine Oracle-MDB auf einem Computer mit dem Betriebssystem Sun Solaris installiert wird, befinden sich die Protokolldateien an den folgenden Speicherorten:

- /tmp/CAInstaller.ca-cms-mdb-schema.install.log
- *CA ITCM-Installationsverzeichnis*/database/setup.log
- *CA ITCM-Installationsverzeichnis*/database/mdb_install/install_*xxxx*.log

Unter Solaris befinden sich auch an den folgenden Speicherorten Protokolldateien:

- *CA ITCM-Installationsverzeichnis*/log/mdbinstall.log
- *CA ITCM-Installationsverzeichnis*/log/mdbupgrade.log

  Falls die Installation zu einem frühen Zeitpunkt fehlschlägt, verbleiben die Protokolldateien möglicherweise unter "/tmp/mdbinstall.log".

MDB-Upgrades

Diese Version unterstützt die folgenden MDB-Upgrades:

- DSM-Manager Version 12.5 oder höher mit entweder lokal oder remote installierter Microsoft SQL Server-MDB.
- DSM-Manager Version 12.5 oder höher mit lokal oder remote auf Solaris, Linux oder Windows installierter Oracle 11g-MDB.
- Gepatchte Version des DSM-Managers und Oracle-MDB, die entweder lokal oder remote unter Windows, Linux und Solaris installiert ist

  Hinweis: Der Oracle 10g-Server muss zunächst auf Oracle 11g R2 aktualisiert werden. Aktualisieren Sie zudem den Oracle-Client auf dem DSM-Manager zu Oracle, bevor Sie das DSM-Manager-Setup starten.

Wenn der Datenbankserver remote ist, wird die MDB während der DSM-Manager-Aktualisierung mit der aktuellen Version aktualisiert. Für Microsoft SQL Server ist keine Benutzerinteraktion erforderlich, da die Datenbankdetails aus dem Comstore abgerufen werden. Legen Sie für Oracle die Umgebungsvariable "ORACLE_HOME" fest, und geben Sie den Namen des Oracle-Dienstes, den TNS-Namen und die "mdbadmin"- und "sys"-Kennwörter ein.

Wenn während des Upgrades vorhandene Datenbanksitzungen erkannt werden, wird jede Sitzung mit dem Namen des Datenbankbenutzers, der Prozess-ID und dem Hostcomputer angezeigt. Die Datenbanksitzungen werden in zwei Listen in einem Dialogfeld angezeigt. Die erste Liste ist für Sitzungen, die geschlossen werden müssen, bevor das Upgrade fortgesetzt werden kann. Diese Liste enthält Sitzungen, die zu Datenbankbenutzern gehören, die Mitglieder von durch das DSM-Schema erstellten Rollen sind. Repräsentative Rollen sind "ams_group", "ca_itrm_group", "ca_itrm_group_ro" (nur Oracle), "ca_itrm_group_ams", "upmuser_group" und "mdbadmin" (nur Oracle). CCE-Rollen (nur für Microsoft SQL Server) (wie "emadmin", "emuser", "uniadmin", "uniuser", "wvadmin" und "wvuser") sind ebenfalls in der ersten Liste enthalten. (Die Rollen werden von einer Konfigurationsdatei auf dem DVD-Image gelesen.)

Die zweite Liste zeigt verbleibende zu anderen Datenbankbenutzern gehörende Sitzungen an. Wir empfehlen, dass Sie auch diese Sitzungen schließen, dieser Schritt ist jedoch nicht obligatorisch. Sie können mit dem Upgrade selbst mit diesen ausstehenden offenen Sitzungen fortfahren.

Verwenden Sie die Schaltfläche "Aktualisieren" in diesem Dialogfeld, um die Listen zu aktualisieren, während Sie offene Datenbanksitzungen schließen. Die Schaltfläche "Fortsetzen" ist nur aktiviert, wenn die erste Liste der Datenbanksitzungen leer ist.

Deinstallation

CA ITCM unterstützt keine Deinstallation des MDB-Schemas. Sie können Datendeinstallationsskript während einer DSM-Manager-Deinstallation verwenden, um ausgewählte Daten aus einer MDB zu entfernen. Sie können auch Microsoft SQL Server- und Oracle-Funktionen verwenden, um MDB-Instanzen zu löschen und erneut zu erstellen.

Besondere Hinweise zu CA ITCM-Installationen

Im Folgenden werden Hinweise und Empfehlungen zu speziellen Installationsszenarien dargestellt. Dieser Abschnitt richtet sich an erfahrene Benutzer.

Einstellungen der Sicherheitsrichtlinie

Die folgenden Sicherheitsrichtlinien müssen für die Benutzeranmeldung aktiviert sein, die zum Installieren des DSM-Managers oder der Management-Datenbank (MDB) verwendet wird.

- Auf diesen Computer über das Netzwerk zugreifen
- Als Teil des Betriebssystems handeln
- Anmeldung über Terminaldienste zulassen
- Als Dienst anmelden

Sie können diese Richtlinien in der Windows-Systemsteuerung über "Verwaltung", "Lokale Sicherheitsrichtlinie" aktivieren.

Neustart von CAM und SSA PMUX

Unabhängig davon, ob Sie Extended Network Connectivity (ENC) installieren möchten, ruft das CA ITCM-Installationsprogramm intern das CA Message Queuing (CAM) und das Secure Socket Adapter Port Multiplexer (SSA PMUX)-Installationsprogramm auf, wodurch bei Bedarf CAM und SSA PMUX neu gestartet werden.

Hinweis: Der SSA PMUX-Neustart gilt nur für Windows.

Weitere Informationen zu ENC finden Sie im Kapitel "Extended Network Connectivity (ENC)".

Verfügbarkeit des Softwareinventars

Direkt nach einer Domänen-Manager-Installation steht nicht das vollständige Softwareinventar zur Verfügung, da der Import der Software-Definitionen in die MDB über eine Engine-Task erfolgt, deren Ausführung standardmäßig für Mitternacht geplant ist.

Installation von DSM-Manager mit einer Remote-SQL Server-MDB über IPV6

Wenn Sie den DSM-Manager (Domäne oder Enterprise) bei einer Remote-SQL Server-MDB über IPv6 registrieren, führen Sie vor der Installation die folgenden Schritte aus:

1. Setzen Sie auf dem Manager-Computer den Wert des folgenden Registrierungsschlüssels auf 1:

   `HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)`

2. Stellen Sie Folgendes sicher:
   - Der Hostname des MDB-Computers wird in eine globale IPv6-Adresse aufgelöst.
   - Die Inverssuche der IPv6-Adresse wird in den gleichen MDB-Hostnamen aufgelöst
3. Stellen Sie sicher, dass der MDB-Computer nur in erreichbare IPv6-Adressen auf dem DSM-Manager-Computer aufgelöst wird, über den der MDB-Computer erreicht wird.

   Dies bedeutet, dass Sie jede IPv4-DNS-Aufzeichnung für den MDB-Computer auf den DNS-Servern, die der Manager-Computer verwendet, sowie alle IPv6-DNS-Datensätze mit Adressen, die der Manager-Computer nicht zum Verbinden mit dem MDB-Computer verwenden kann, löschen müssen. Der DNS-Cache auf dem DSM-Manager muss ordnungsgemäß gelöscht werden. Sonst kann JDBC keine Verbindung mit der MDB herstellen, wodurch die Installation von CCS, CIC und MDB-Java-Komponenten beeinflusst wird.

Installation von Domänen-Manager mit Hilfe einer Remote-SQL Server-MDB mit einer benannten Instanz

Stellen Sie für eine erfolgreiche Installation des Domänen-Managers mit Hilfe einer Remote-SQL Server-MDB mit einer benannten Instanz sicher, dass der SQL Server-Browser auf dem Remote-MDB-System ausgeführt wird. Stellen Sie vor der Installation sicher, dass der Domänen-Manager eine Verbindung zur Remote-MDB herstellen kann, und dass der Microsoft SQL-Browser ordnungsgemäß funktioniert, indem Sie auf dem Domänen-Manager-System den folgenden Befehl ausführen:

```
sqlcmd -E -d mdb -S MDB-Servername [\Instanzname] -q "select * from mdb"
```

Installation des eigenständigen Remote Control-Agenten

Die Remote Control (RC)-Funktion von CA ITCM kann im Standalone-Modus konfiguriert werden. In diesem Modus nutzt der RC-Agent die lokalen Sicherheits- und Konfigurationsrichtlinien statt der Richtlinien, die von einem zentralen Domänen-Manager gesendet werden.

Der CA ITCM-Installationsdatenträger (DVD) enthält einen gesonderten Installationsassistenten mit der Bezeichnung "setup_rc", mit dem ein eigenständiger RC-Agent installiert werden kann.

Die Installation des eigenständigen RC-Agenten aktiviert nur die folgenden CAF-Plug-ins:

- pmux
- rchost
- smserver

"setup_rc" finden Sie unter:

- WindowsProductFiles_x86\AgentRC
- LinuxProductFiles_x86/rc_agent

Installation auf Solaris Intel

Bevor Sie mit der Installation von CA ITCM auf der Solaris- (Intel) Plattform beginnen, stellen sie sicher, dass die folgenden Patches für das SUNWlibC-Paket installiert sind:

- 109148-07
- 108436-16

Diese Patches stellen sicher, dass Standard-C++ Laufzeit-Bibliotheken vorhanden sind.

Sie können das Vorhandensein dieser Patches mit dem folgenden Befehl überprüfen:

```
showrev –p | grep SUNWlibC
```

Dabei erscheint die folgende Ausgabe:

```
Patch: 108436-16 Obsoletes: Requires: 109148-07 Incompatibles: Packages: SUNWlibC
```

Hinweis: Client-Automatisierung hängt von CAPKI ab, und CAPKI hat eine Abhängigkeit von "libucb" unter Solaris Intel. Wenn "libucb" auf Solaris Intel 11 nicht standardmäßig installiert ist, dann schlägt die Installation fehl.

Führen Sie diese Schritte aus, um "libucb" unter Solaris Intel 11 zu installieren:

1. Führen Sie folgenden Befehl aus, um das Paket zu identifizieren.

   pkg search -r /usr/ucblib/libucb.so.1

2. Führen Sie folgenden Befehl aus, um das Paket zu installieren.

   pkg install <package name>

Umgebungsvariable PATH für Solaris Intel

Beim Start der Shell werden die Startskripte aufgerufen. Beachten Sie, dass sh-basierte Shells (wie "Bash") "/etc/profile" und dann "~/.profile" aufrufen. Die Solaris 11 Intel ~/.profile für den Root-Benutzer überschreibt jedoch die Umgebungsvariable PATH.

Wenn PATH keine CA Pfade enthält, stellen Sie sicher, dass Sie das Startskript in der folgenden Weise mit dem Befehl "source" aufrufen:

- . /etc/profile.CA all oder
- source /etc/csh_login.CA all

Zugriff auf den VMware-ESX-Webservice

Um auf den VMware-ESX-Webservice zuzugreifen, müssen Sie die folgenden Anmeldeinformationen für den Benutzer eines VMware-ESX-Hostrechners angeben:

Hostname

Gibt den Namen des ESX-Hosts an, für den Asset Management-Inventar erfasst werden soll. Eine IP-Adresse kann auch angegeben werden.

Webservice-Benutzername

Gibt den Namen eines VMware-ESX-Benutzers an, der die VMware-Systemrolle des Administrators oder Schreibgeschützt hat.

Webservice-Kennwort

Erfordert das Kennwort für den angegebenen VMware-ESX-Benutzer.

Webservice-URL

Zeigt die URL des Webservice an, die das folgende Format hat:

`https://ESXHostFQDNservername/sdk`

ESXHostFQDNservername stellt den voll qualifizierten Hostnamen des ESX-Servers dar. Alternativ kann eine IP-Adresse an Stelle des Hostnamens angegeben werden.

ESX-Inventarsammlung wird unter Verwendung der Webservice-Engine (SOAP) durchgeführt. Standardmäßig wird der Webservice als sicherer Webservice auf Port 443 ausgeführt, auf den unter Verwendung von SSL über HTTPS zugegriffen werden kann.

Installation der Remote Control-Komponente unter Linux

Die Remote Control (RC)-Funktion von CA ITCM unterstützt Linux. Diese Betriebsumgebung unterstützt nur die RC-Hostkomponente.

Wenn der eigenständige RC-Agent für diese Betriebsumgebung benötigt wird, muss er aus dem Verzeichnis "LinuxProductFiles_x86/rc_agent" installiert werden.

Eigenständige Agenten können nicht mit der Software Delivery-Funktionalität oder dem interaktiven Installer bereitgestellt werden.

Installation der Remote Control-Komponente auf Apple Mac OS X

Die Remote Control-Funktion von CA ITCM unterstützt Apple Mac OS X. Diese Betriebsumgebung unterstützt nur die Remote Control-Hostkomponente.

Der Modus "Sichere Steuerung" wird nicht unterstützt. Alle anderen Steuerungsmodi (Verdeckte Ansicht, Ansicht, Freigegeben, Interaktiv und Exklusiv) werden unterstützt.

Wie mit Linux haben die Viewer-Option "Host-Hintergrundbild deaktivieren" und andere Funktionalitäten für den Benutzer keine Auswirkungen.

Wichtig! Nachdem Sie einen Remote Control-Agenten auf einer Mac OS X-Plattform installiert, neu installiert, repariert oder aktualisiert haben, wird empfohlen, dass Sie sich vom System abmelden und wieder anmelden. Dies stellt sicher, dass wichtige DSM-Prozesse im richtigen Benutzerkontext gestartet werden. Wenn dieser Schritt ausgelassen wird, werden Versuche einer Remote Control-Verbindung mit folgender Meldung abgelehnt: "Der Host konnte den Desktop des aktuellen Benutzers nicht öffnen."

Freigabezugriff für Boot-Server

Der Boot-Server wird immer als Teil eines Scalability-Servers installiert. Die Konfigurationsdetails des Boot-Servers werden auf den Seiten zur Scalability-Server-Konfiguration des Installationsassistenten angegeben.

Wenn Sie statt TFTP (Standardeinstellung) einen Freigabezugriff benötigen, klicken Sie auf der Seite "Scalability-Server konfigurieren" im Bereich "Erweiterte Serverkonfiguration" auf die Schaltfläche "Boot-Server" und wählen Sie die Option "Unterstützung für Windows-Netzwerkfreigaben aktivieren". Das Installationsprogramm erstellt schreibgeschützte Netzwerkfreigaben, auf die über das SMB-Protokoll zugegriffen werden kann.

Weitere Informationen zum Wechseln von TFTP zum Freigabezugriff und zum Deaktivieren des PXE-Servers finden Sie im *BS-Installationsverwaltung-Administrationshandbuch* in der Online-Dokumentation zu CA IT Client Manager (Bookshelf).

Domänen-Controllerverbindung bei der Installation von CCS

Wenn die Verbindung zum Domänen-Controller bei der Installation von CCS als Domänenadministrator getrennt wird, tritt bei der CCS-Installation beim Validieren der Rechte des installierenden Benutzers ein Fehler auf. In manchen Fällen wird der Rückgabe-Code "1073741819" angezeigt.

Sie können dies beheben, indem Sie die Verbindung zum Domänen-Controller wiederherstellen, oder die Installation als lokaler Administrator durchführen.

Verschiebevorgänge der Agent- und Scalability-Server

Ein Agent ist so konfiguriert, dass immer nur ein Domänen-Manager zur selben Zeit verbunden ist. Der Agent kann allerdings neu konfiguriert werden. Das Verschieben eines Agenten kann durch den folgenden Befehl ausgelöst werden:

```
caf setserveraddress new_scalability_server
```

Das Verschieben eines Scalability-Servers kann durch den folgenden Befehl ausgelöst werden:

```
cserver config -h new_domain_manager
cserver register
```

Wenn ein Kalender auf einem CA Common Services-Server CCS aktualisiert wird (der sich auf einem DSM-Manager befindet), müssen die CCS-Agenten (auf den DSM-Scalability-Servern) aktualisiert werden. Führen Sie deshalb die Scalability-Server-Prozedur "CCS-Kalender synchronisieren" auf jedem untergeordneten Scalability-Server aus, auf dem ein CCS-Agent installiert ist.

Wenn Sie einen Scalability-Server mit Hilfe des Befehls "cserver config -h Neuer_Manager" von einem Manager zu einem anderen verschieben, wird der CCS-Agent auf diesem Scalability-Server automatisch neu konfiguriert, damit er sich mit dem neuen Manager verbindet.

Hinweis: Um sicherzustellen, dass CCS-Werte nicht verändert werden, wenn man den Server erneut registriert, verwenden Sie den Befehl "cserver" mit der Option "-i" statt der Option "-h".

Wird der Server jedoch mit Hilfe von Richtlinien verschoben, muss dies manuell geschehen, da der Agent sich sonst weiterhin manuell mit dem alten CCS-Server verbindet. Um den CCS-Server auf dem neuen_Manager einzustellen, führen Sie auf dem Scalability-Server folgenden Befehl aus:

```
cautenv setlocal CA_CALENDAR_NODE neue_Manageradresse
cautenv setlocal CA_OPR_PROXY neue_Manageradresse
unicntrl stop all
unicntrl start all
```

DSM-Manager mit CCS WorldView-Manager oder Installation von CCS einschließlich MDB auf einem Domänen-Controller

In diesem Installationsszenario (DSM-Manager mit CA Common Services CCS WorldView-Manager oder Installation von CCS einschließlich MDB auf einem Domänen-Controller) gilt folgende CCS-Einschränkung:

Der CCS WorldView-Manager kann nicht auf einem als Domänen-Controller vorgesehenen Server installiert werden.

Dies liegt daran, dass die IPSEC-Sicherheitsrichtlinien Vorrang vor den Benutzerrechten für den Microsoft COM-Server haben, wenn das CA Severity Propagation COM-Objekt gestartet wird.

Aufgrund dieser Einschränkung kann CA IT Client Manager den CCS WorldView-Manager nicht auf einem Domänen-Controller installieren. Dies betrifft den DSM-Manager und die Installation von CCS einschließlich MDB. Für eine ordnungsgemäße Installation des DSM-Managers auf einem Domänen-Controller gibt es folgende Möglichkeiten:

- CCS deaktivieren (dann ist keine CCS-Funktionalität verfügbar)
- Remote-Installation von MDB und CCS (dann wird CCS WorldView-Manager MDB-seitig installiert)

Installation eines Scalability-Servers unter Linux

Wenn ein Scalability-Server unter Linux, unter Verwendung von DMDeploy oder Software-Delivery mit dem CA DSM Scalability Server Linux (Intel) DEU-Paket, installiert ist, ist die CA Common Services-Software *nicht* installiert. Wenn CCS mit einem Scalability Server unter Linux erforderlich ist, dann muss es interaktiv von der DVD installiert werden.

Installation und Registrierung von UNIX- und Mac OS X-Komponenten

Diese Komponenten werden bei der Installation des Domänen-Managers nicht automatisch in den Software Delivery- und Infrastructure Deployment-Bibliotheken registriert.

Um diese Pakete auf dem Domänen-Manager zur Verfügung zu stellen, importieren Sie sie mit Hilfe des Tools "dsmPush" (Datei "dsmPush.dms" im Stammverzeichnis der DVD) von der entsprechenden CD in die Softwarepaketbibliothek und in den Infrastructure Deployment-Payload-Bereich des Managers.

Führen Sie folgenden Befehl aus:
`dmscript dsmPush.dms copy -I` *`Speicherort_des_CD_Image`*

Um diese Pakete in der Softwarepaketbibliothek zu registrieren, können Sie sie auch von der entsprechenden CD kopieren und in den Ordner "Software-Bibliothek" des DSM-Explorers einfügen.

Besonderheiten bei UNIX-Agenten

Die derzeit durch den UNIX-Agenten in CA ITCM unterstützte UNIX-Betriebsumgebungen werden in der im CA ITCM-Bookshelf oder auf CA-Support verfügbaren Kompatibilitätsmatrix aufgelistet. Auf den dort genannten Plattformen kann auch der Packager für Linux und UNIX ausgeführt werden.

Installationsvoraussetzungen für den Agenten unter Sun Solaris

Bevor Sie den UNIX-Agenten auf einem Sun Solaris-Computer installieren, müssen Sie sicherstellen, dass die erforderlichen minimalen Kernel-Konfigurationsparameter festgelegt wurden.

So legen Sie die Kernel-Konfigurationsparameter für Solaris 5.10 fest oder ändern sie:

Für Solaris 5.10 muss der Konfigurationsparameter zur Ressourcenkontrolle "max-shm-memory" auf 5242880

oder höher festgelegt sein. Der Parameter "max-sem-ids" muss auf 256 oder höher festgelegt sein.

1. Fragen Sie die aktuellen Werte dieser Parameter mit Hilfe des Befehls "prctl" ab, z. B.:

   ```
   prctl –P –n project.max-shm-memory –i project user.root
   ```

   ```
   prctl –P –n project.max-sem-ids –i project user.root
   ```

2. Verwenden Sie *einen* der folgenden Befehle, wenn die Ressourcensteuerungs-Konfigurationsparameter aktualisiert werden müssen:

   - Verwenden Sie "prctl", um Ressourcensteuerungs-Konfigurationsparameter zu ändern, z. B.:

     ```
     prctl -n project.max-shm-memory -v 5242880 -r -i project user.root
     ```

     ```
     prctl -n project.max-sem-ids -v 256 -r -i project user.root
     ```

     Hinweis: Konfigurationsparameter, die mit Hilfe des Befehls "prctl" geändert wurden, sind *nicht* dauerhaft geändert, und Sie müssen die Befehle nach einem Neustart des Computers erneut ausführen.

   - Verwenden Sie "projmod", um Ressourcensteuerungs-Konfigurationsparameter zu ändern, z. B.:

     ```
     projmod -s -K "project.max-shm-memory=(priv,5242880,deny)" user.root
     ```

     ```
     projmod -s -K "project.max-sem-ids=(priv,256,deny)" user.root
     ```

     Hinweis: Konfigurationsparameter, die mit Hilfe des Befehls "projmod" geändert wurden, sind nach einem Neustart des Computers dauerhaft geändert.

Installationsvoraussetzungen für den Agenten unter IBM AIX

Wenn Sie den CA ITCM UNIX-Agenten auf einem IBM AIX-Computer mit AIX Version 5.3 und höher installieren, werden die neuesten Laufzeitumgebungsbibliotheken von IBM installiert.

Software Delivery-Download und UNIX-Agenten

Die folgenden Hinweise sind zu beachten, wenn als Download-Methode für Software Delivery die Methode "Intern - NOS" verwendet wird.

Der Sun Solaris-Kernel unterstützt derzeit nicht das Mounten von Samba-Freigaben.

Wenn auf dem Scalability-Server nur NFS-Bereitstellungspunkte konfiguriert sind (er also kein Samba verwendet), verwenden die Sun Solaris-Agenten automatisch NFS.

Wenn auf dem Scalability-Server Samba-Freigaben konfiguriert sind und der Parameter "NOSLessSwitchAllowed" auf 1 (Wahr) gesetzt ist, verwenden die Sun Solaris-Agenten die Download-Methode "Intern - ohne NOS".

Wenn auf dem Scalability-Server Samba-Freigaben konfiguriert sind und der Parameter "NOSLessSwitchAllowed" auf 0 (Falsch) gesetzt ist, schlägt der Download auch fehl, wenn auf dem Scalability-Server auch NFS-Bereitstellungspunkte konfiguriert sind.

Der aktuelle Wert des Parameters "NOSLessSwitchAllowed" kann durch Ausführen des folgenden Befehls verifiziert werden:

```
ccnfcmda -cmd GetParameterValue -ps itrm/usd/agent -pn NOSLessSwitchAllowed
```

Der aktuelle Wert des Parameters "NOSLessSwitchAllowed" kann durch Ausführen des folgenden Befehls auf 1 gesetzt werden:

```
ccnfcmda -cmd SetParameterValue -ps itrm/usd/agent -pn NOSLessSwitchAllowed -v 1
```

Hinweis: Für ausführlichere Information über den Ccnfcmda-Befehl zur Agentenkonfiguration tippen Sie "<command> /?" in der Befehlszeile eingeben.

Hinweis zur Data Transport Service-Installation

Unter Windows befindet sich die Data Transport Service-Funktionalität (DTS) nicht im Software Delivery (SD)-Agenten-Plug-in, sondern in einem separaten Installationspaket. D. h., dass Sie das gesonderte DTS-Installationspaket auf diesem Agenten bereitstellen müssen, wenn Sie die DTS-Funktionalität benötigen, z. B. um die Download-Methode für diesen bestimmten Agenten anzugeben.

Unter Linux oder UNIX ist die Data Transport Service-Funktionalität im Software Delivery (SD)-Plug-in enthalten, d. h., DTS wird mit dem SD-Agenteninstallationspaket installiert.

Umbenennen von Managern und Scalability-Server-Computern

CA IT Client Manager (CA ITCM) unterstützt das Umbenennen von Enterprise-Managern und Domänen-Managern über das entsprechende Dialogfeld "Domäne" oder "Enterprise-Eigenschaften". Die Felder "Name", "Kontaktinformationen" und "Beschreibung" können bearbeitet werden. Ihre Werte werden zwischen dem Domänen- und dem Enterprise-Manager repliziert.

CA ITCM unterstützt jedoch nicht das Umbenennen von Scalability-Server-Computern.

Systemnamen als vollständig qualifizierte Domänennamen

Wenn der CA ITCM-Installer zur Eingabe eines Systemnamens auffordert, wird Ihnen dringend empfohlen, einen vollständig qualifizierten Domänennamen (FQDN) einschließlich Domänensuffix einzugeben, so dass Computersysteme in anderen Netzwerkdomänen erreichbar sind, auch wenn die Anforderungsweiterleitung nicht für alle beteiligten DNS konfiguriert ist.

Installation von CA ITCM bei vorinstalliertem Unicenter NSM r11

Wenn Unicenter NSM r11 vor CA IT Client Manager installiert wird, müssen vor Beginn der CA IT Client Manager-Installation folgende CCS-Komponenten von Unicenter NSM installiert werden:

Unicenter NSM-Komponenten:

- Managementdatenbank
  - MDB für Microsoft SQL Server
- WorldView
  - Admin-Client
  - WorldView Manager
- Enterprise-Management
  - Admin-Client
  - Event Management
    - Ereignis-Agent
    - Ereignis-Manager
- Continuous Discovery
  - Continuous Discovery-Agent
  - Continuous Discovery-Manager

Starten Sie die Unicenter NSM-Installation, überprüfen Sie, ob alle aufgeführten Komponenten installiert sind, und installieren Sie alle fehlenden Komponenten.

Nach Abschluss der Installation von Unicenter NSM können Sie die Installation von CA IT Client Manager starten.

Angeben der Port-Nummer für die Webkonsole während der Installation

Die Änderung des SQLServer.PortNo-Schlüssels mit der Datenbank-Portnummer in der Datei "wacconfig.properties" ist mit der Unterstützung mehrerer Manager in der Webkonsole nicht länger gültig. Während der Installation muss die richtige Portnummer angegeben werden. Eine Änderung zu einem späteren Zeitpunkt ist nicht möglich.

Hinweis zum Hinzufügen der Webkonsole mit Hilfe der Methode zum Ändern der Installation

Wenn Sie die Webkonsole mit Hilfe der Methode zum Ändern der Installation hinzufügen, müssen Sie sicherstellen, dass mindestens 8 GB Speicherkapazität auf der Festplatte verfügbar sind.

Deaktivieren des Virenschutzes während Installation und Deinstallation

Es wird empfohlen, dass Sie die Virenschutzsoftware deaktivieren, bevor Sie eine CA IT Client Manager-Installation oder -Deinstallation starten. Wenn die Virenschutzsoftware aktiviert bleibt, können Interferenzen mit dem Installations- oder Deinstallationsprozess auftreten.

Deaktivieren des Remote-Sektorserver-Dienstes während der Installation

Wenn auf dem Computer, auf dem Sie CA ITCM installieren möchten, ein Remote-Sektorserver (RSS) einer früheren Unicenter Asset Management-Version installiert ist, muss der RSS-Dienst beendet werden, bevor Sie die CA ITCM-Installation starten. Der RSS-Dienst muss deaktiviert werden, da er automatisch versucht, neu zu starten.

Deaktivieren Sie den Asset Management-Sektorserver-Dienst über den Dienststeuerungs-Manager. Aktivieren Sie den Dienst nach der Installation erneut.

Windows XP-Netzwerkzugriff - Modell für gemeinsame Verwendung und Sicherheitsmodell für lokale Konten

Wenn diese Windows XP-Richtlinie auf "Nur Gast" eingestellt ist, werden Benutzer, die sich als lokaler Benutzer authentifizieren, dem standardmäßig aktivierten Gastkonto zugeordnet. In der Folge schlägt die Authentifizierung fehl.

Um dieses Problem zu beheben, konsultieren Sie die Microsoft-Dokumentation unter:

www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/506.mspx

Betrachtungen zu Windows Server 2003

Auf Windows NT- und Windows 2000-Servern konnte für den Zugriff auf Netzwerkressourcen standardmäßig der anonyme Zugriff, auch als NULL-Sitzungen bezeichnet, verwendet werden. Dateisystemfreigaben (NULL-Sitzungsfreigaben) konnten so konfiguriert werden, dass sie NULL-Sitzungen akzeptieren. Für Software Delivery (SD)-Agenten, die über das Konto "LocalSystem" ausgeführt werden, war dies schon immer die bevorzugte Art des Zugriffs auf die Softwarepaketbibliothek (SDLIBRARY$ -Freigabe) auf dem Scalability-Server.

Mit Windows Server 2003 hebt Microsoft die Sicherheitsstufe im Vergleich zu den Vorgängerversionen des Serverbetriebssystems an. Anonymer Zugriff und NULL-Sitzungsfreigaben sind standardmäßig deaktiviert. Die Notwendigkeit des anonymen Zugriffs wurde für Computer, die der Domäne angehören, eliminiert, indem Computerdomänenkonten im Windows-Sicherheitssystem zu echten Sicherheitsprinzipalen gemacht wurden. In Windows 2000-Domänen und später in Windows Server 2003-Domänen können Zugriffsrechte sowohl Computerkonten als auch Benutzerkonten gewährt werden.

Bei Windows Server 2003 werden keine NULL-Sitzungsfreigaben verwendet, um diesen Agenten Zugriff auf die Softwarepaketbibliothek zu bieten. Stattdessen verlässt sich SD darauf, dass Agenten über ihre Computerdomänenkonten der Zugriff auf die Bibliothek gewährt wird. Dieser Ansatz, auch wenn er sicherer ist und mit den Empfehlungen von Microsoft im Einklang steht, bietet keine vollständige Lösung für alle unterstützten SD-Agentenplattformen.

Zur Entwicklung des anonymen Zugriffs in Windows-Betriebsumgebungen lesen Sie bitte Artikel 278259 in der Knowledge Base von Microsoft Support.

Administrative MSI-Installation mit SDMSILIB auf Windows Server 2003

Wenn Sie die Pakete in der SDMSILIB-Freigabe mit einer administrativen MSI-Installation bereitstellen, reicht die Methode "sd_sscmd libraryaccess" nicht für den Aufbau einer Verbindung zu dieser Freigabe aus. Die Agenten müssen in der Lage sein, auf diese Freigabe zugreifen zu können, auch wenn keine Installationen oder Konfigurationen ausgeführt werden, die die Software Delivery (SD)-Funktionalität verwenden. Die Ursache hierfür ist, dass Zugriffsanforderungen an die SDMSILIB-Freigabe jederzeit von MSI-Installationen angefordert werden können, z. B. wenn Reparaturen oder Selbstreparaturen ausgeführt werden. Stattdessen verlässt sich SD darauf, dass Agenten über ihre Computerdomänenkonten der Zugriff auf die SDMSILIB-Freigabe gewährt wird.

Windows 2003 SP1-MSI-Bibliothekszugriff - Anonymen Zugriff auf Named Pipes und Freigaben einschränken.

Der anonyme Zugriff auf Netzwerkfreigaben wird bei Windows 2003 Service Pack 1 standardmäßig verweigert.

Für Netzwerkinstallationen von MSI-Paketen aus der SDMSILIB-Freigabe oder allgemein anonymen Zugriff auf die SDLIBRARY$-Freigabe auf einem Computer mit Windows 2003 Service Pack 1 müssen folgende Schritte ausgeführt werden:

- Legen Sie folgende Sicherheitsoption in der lokalen Sicherheitsrichtlinie fest: 'Netzwerkzugriff: Anonymen Zugriff auf Named Pipes und Freigaben einschränken: Deaktiviert" ein.
- Starten Sie das System erneut, damit die Änderungen wirksam werden.

Verbinden von SD-Agenten mit SD-Scalability-Servern

Folgendes gilt nur, wenn Software Delivery (SD)-Agenten eine Verbindung zu SD-Scalability-Servern herstellen, die unter Windows Server 2003 ausgeführt werden, und wenn die lokale Sicherheitsrichtlinie "Netzwerkzugriff: Anonymen Zugriff auf Named Pipes und Freigaben einschränken" auf dem Manager des Scalability-Servers auf "Aktiviert" eingestellt ist.

SD-Agenten, die auf Computern mit Windows XP oder Windows Server 2003 ausgeführt werden, wird ebenfalls der Zugriff verweigert, wenn sie keiner oder einer anderen, nicht vertrauenswürdigen Domäne angehören als der SD-Manager, auf dem sich die Freigabe der Softwarepaketbibliothek befindet.

Um diese Zugriffsprobleme für SD-Agenten unter Windows XP oder Windows Server 2003 zu lösen, kann manuell ein dediziertes Benutzerkonto auf dem Scalability-Servercomputer erstellt und der Gruppe "Jeder" hinzugefügt werden. Damit wird schreibgeschützter Zugriff auf die SDLIBRARY$-Freigaben gewährt. In den allgemeinen Konfigurationsspeicher der einzelnen Domänen-Manager und Scalability-Server, die auf der neuen Windows-Managerplattform ausgeführt werden, müssen der Benutzername und das Kennwort eingegeben werden.

SD-Agenten nutzen automatisch den internen Download ohne NOS, um Fehlfunktionen zu vermeiden, wenn der Zugriff auf die Bibliothek verweigert wird. Dieses Verhalten kann optional ausgeschaltet werden, indem Sie in der Konfigurationsrichtlinie im Abschnitt "itrm/usd/agent" die Einstellung "NOSLessSwitchAllowed" auf "False" einstellen.

Windows Server 2008 Core-Betriebsumgebungen

Dieser Abschnitt beschreibt bekannte Probleme, Problembehebungen und Lösungen, die auf Windows Server 2008 Server Core-Betriebsumgebungen anwendbar sind.

Abhängigkeit von der graphischen Benutzeroberfläche (GUI)

Windows Server 2008 Server Core bietet eingeschränkte GUI-Funktionen. Aufgrund der Abhängigkeit von der GUI werden die folgenden CA ITCM-Agent-Optionen nicht unterstützt:

- Remote Control-Chat
- Remote Control-Viewer
- Softwarekatalog
- SysTray

Abhängigkeit von IE

Windows Server 2008 Server Core unterstützt aufgrund der Abhängigkeit von IE keine HTML-basierten Installationsprogramme.

Um die CA ITCM-Agenten zu installieren, wählen Sie *eine* der folgenden Möglichkeiten:

- Gehen Sie vom Installationsmedium direkt zum Verzeichnis "WindowsProductFiles" und führen Sie "setup.exe" aus.
- Verwenden Sie DMDeploy, um die Agent-Plugins aus dem DSM Explorer heraus bereitzustellen.

Deinstallieren Sie die Agenten

Windows Server 2008 Server Core bietet keine Unterstützung für Programme zum Hinzufügen oder Entfernen. Um die Agenten zu deinstallieren, führen Sie "msiexec" auf der Befehlszeile aus.

Weitere Informationen zur Verwendung von msiexec finden Sie im Abschnitt Installationstool msiexec (siehe Seite 173).

Nicht unterstützte Optionen

Windows Server 2008 Server Core unterstützt nicht:

- Online-Hilfe für Agenten
- Ausführungsmodus "Abmeldung des Benutzers erzwingen, bevor der Job ausgeführt wird" des Logon Shield
- Die Option "Logoff" der Prozeduroptionen "Boot-Ebene vor der Ausführung" und "Boot-Ebene nach der Ausführung"

Hinweise zu Firewall und Ports

Einige Betriebssysteme, z. B. Windows XP und Red Hat, enthalten eine Firewall-Funktion, die verhindern kann, dass Remote-Verbindungen hergestellt werden. Diese Remote-Verbindungen umfassen die Verbindungen von anderen DSM-Komponenten, z. B. Scalability-Servern. Damit CA IT Client Manager einwandfrei funktionieren kann, muss die Firewall eventuell neu konfiguriert werden.

Eine Übersicht der Ports, die derzeit von CA IT Client Manager und den einzelnen Komponenten verwendet werden, wird unter "Von CA IT Client Manager verwendete Ports (siehe Seite 551)" zur Verfügung gestellt.

Kompatibilitätsbibliotheken für Linux

Der DSM-Installer setzt voraus, dass bestimmte abhängige Bibliotheken vorhanden sind. Wenn diese Bibliotheken nicht vorhanden sind, funktionieren die installierten Komponenten möglicherweise nicht einwandfrei.

In der folgenden Tabelle werden die Details der Voraussetzungen für die Softwarebibliothek dargestellt. Diese Bibliotheken müssen vor dem Installieren der DSM-Komponenten auf den Linux-Hosts vorhanden sein.

Linux-Distribution/Version	Erforderliche RPM-Pakete
Red Hat 5 Enterprise Linux	glibc 2.3.3-84 compat-libstdc++ 33-3.2.3-61 Für 64-Bit-Versionen des BS: ncurses 5.4-1.3 (i386) oder ncurses-devel 5.4-13 (i386) zlib 1.1.4-8.1 (i386) oder zlib-devel 1.2.1.2-1.2 (i386)
SuSE Linux Enterprise Server 10	glibc 2.3.3-84 compat 2004.4.2-3 libstdc++ 3.2.2-38

Hinweis: Die neuesten Informationen zu den benötigten Kompatibilitätsbibliotheken und zusätzlichen Systempaketen finden Sie auf der Support-Website Ihres Linux-Anbieters.

MSI-Voraussetzungen für den Installer

In allen Windows-Betriebsumgebungen setzt der CA ITCM-Installer den Microsoft Windows Installer (MSI) Engine 2.0 voraus. Wenn diese Version nicht verfügbar ist, installiert der Installationsassistent ihn automatisch vor einem Installationsschritt. Der Upgrade auf MSI 2.0 erfordert einen Neustart des Systems.

Auf Systemen mit Windows 2003 ist ein Neustart des Systems sehr unwahrscheinlich, da MSI 2.0 als Bestandteil des Betriebssystems installiert sein müsste.

Komponente	Windows-Plattform für Installation	Erwartete MSI-Version	Vom Installer ausgeführte Aktion, wenn die erwartete MSI-Version nicht auf dem Zielcomputer vorhanden ist.
GUI	Alle	2.0	Installieren/Auf Version 2.0 aktualisieren
Manager	Alle	2.0	Installieren/Auf Version 2.0 aktualisieren
Server	Alle	2.0	Installieren/Auf Version 2.0 aktualisieren
Agent	2003	2.0	Installieren/Auf Version 2.0 aktualisieren

Hinweis: Wenn Agenten mit der Software Delivery- oder Infrastructure Deployment-Funktionalität installiert werden, müssen Sie sicherstellen, dass der Microsoft Windows Installer bereits auf den Zielcomputern installiert ist. Bei Bedarf können Sie den Microsoft Windows Installer von der Microsoft-Website herunterladen (www.microsoft.com).

Gemeinsame Verwendung der MDB durch CA Service Desk Manager und CA ITCM

Wenn Sie möchten, dass CA Service Desk Manager und CA ITCM dieselbe MDB verwenden, müssen Sie zuerst CA Service Desk Manager und anschließend CA ITCM installieren.

Administrative Installation unter Windows

Dies ist eine manuelle Installationsoption, die nur für Windows-Betriebsumgebungen gilt. In einer administrativen Installation kann der Microsoft Windows Installer den Inhalt des Installations-Images dekomprimieren und das dekomprimierte Image in eine Netzwerkfreigabe kopieren.

Installationsverzeichnisse unter Windows

Im Folgenden werden die Struktur der Installationsverzeichnisse in Windows-Umgebungen und die Regeln und Einschränkungen für sie beschrieben:

Standardmäßiger Basispfad

`C:\Programme\CA\DSM`

Sie können diesen standardmäßigen Basispfad ändern, wenn Sie dazu aufgefordert werden.

Pfad für freigegebene Komponenten

Freigegebene Komponenten werden in unterschiedlichen Verzeichnissen installiert. Der Windows-Installer erstellt standardmäßig Verzeichnisse für alle freigegebenen Komponenten unter folgendem Basispfad:
`C:\Programme\CA\SC`

Sie können diesen standardmäßigen Basispfad ändern, wenn Sie dazu aufgefordert werden.

Umgebungsvariable "PATH"

Während der Installation wird die Umgebungsvariable PATH erweitert um

Basispfad`\bin`

Im folgenden Fall wird die Umgebungsvariable PATH jedoch während der Installation nicht automatisch aktualisiert:

Wenn Sie die Installation über eine Terminalserversitzung vornehmen, wird die Änderung an der Variable "PATH" nur wirksam, wenn eine der folgenden Aktionen abgeschlossen wurde:

- Abmelden und erneutes Anmelden beim System
- Neustart des Systems

Dieses Verhalten wird vom Microsoft-Betriebssystem verursacht und kann daher nicht geändert werden.

In der Folge kann die Befehlszeilenschnittstelle des Application Frameworks (CAF) auf einigen Windows-Systemen erst verwendet werden, wenn Änderungen an der Variable "PATH" erkannt wurden.

Die maximale Länge der Variable "PATH" wird von der verwendeten Windows-Betriebsumgebung festgelegt. Während der Installation wird die tatsächliche Länge der Variable "PATH" geprüft. Wenn aufgrund der Länge keine zusätzliche Verzeichnisnamen hinzugefügt werden können, wird der Installationsprozess beendet.

Installationsverzeichnisse unter Linux und UNIX

Im Folgenden werden die Struktur der Installationsverzeichnisse von CA ITCM in Linux- und UNIX-Umgebungen und die Regeln und Einschränkungen für sie beschrieben:

Standardmäßiger Basispfad

Das standardmäßige CA ITCM-Installationsverzeichnis ist:
`/opt/CA/DSM`

Auf das CA ITCM-Installationsverzeichnis verweist auch die Umgebungsvariable "$CA_ITRM_BASEDIR".

Sie können diesen standardmäßigen Basispfad ändern, wenn Sie dazu aufgefordert werden.

Pfad für freigegebene Komponenten

Freigegebene Komponenten werden in unterschiedlichen Verzeichnissen installiert. Der Installer erstellt standardmäßig Verzeichnisse für alle freigegebenen Komponenten unter folgendem Basispfad:
`/opt/CA/SharedComponents`

Auf den Speicherort der allgemeinen Komponenten verweist auch die Umgebungsvariable "$CASHCOMP", die vom Installer eingerichtet wird.

Hinweis: "$CASHCOMP" wird von allen CA-Produkten auf einem Computer gemeinsam verwendet. Wenn dieser Wert festgelegt wurde (durch vorheriges Installieren anderer CA-Produkte), kann er in der CA ITCM-Installation nicht geändert werden. Der Installer berücksichtigt die bestehenden Einstellungen.

Umgebungsvariable "PATH"

Sie können angeben, ob die systemweite Umgebungsvariable "PATH" am Ende der Installation aktualisiert werden soll oder nicht. Wenn Sie diesen Vorgang unterlassen, können Sie den Pfad noch nach der Installation manuell mit den Umgebungsvariablen einrichten, die zum ordnungsgemäßen Betrieb von CA ITCM erforderlich sind. Um diesen Vorgang in einer Bourne/Korn/Bash-Shell auszuführen, führen Sie folgenden Befehl aus:

```
# . $CA_ITRM_BASEDIR/scripts/ITRMenv
```

Zum Einrichten der Umgebung in der C-Shell führen Sie folgenden Befehl aus:

```
# source $CA_ITRM_BASEDIR/scripts/ITRMenvcsh
```

Installieren des Alarm-Collector

Sie können die Rolle festlegen, in der der Alarm-Collector zum Zeitpunkt der Bereitstellung ausgeführt werden muss. Konfigurieren Sie den Alarm-Collector für eine der folgenden Rollen:

Alarme in der MDB beibehalten

Konfiguriert den Alarm-Collector so, dass Alarme in der MDB beibehalten werden.

Alarme in der MDB beibehalten und konfigurierte Aktionen ausführen

Konfiguriert den Collector so, dass Alarme in der MDB beibehalten werden und konfigurierte Aktionen wie das Senden von E-Mails, das Erstellen von SNMP-Traps und das Schreiben in Windows/CCE-Ereignisprotokoll durchgeführt werden.

Alarme beibehalten, Aktionen ausführen und sie weiterleiten

Konfiguriert den Collector so, dass Alarme in der MDB beibehalten, konfigurierte Aktionen durchgeführt und Alarme in einen anderen Alarm-Collector weitergeleitet werden.

Weiterleiten

Konfiguriert den Collector für die Weiterleitung von Alarmen in einen anderen Alarm-Collector.

Installieren Sie den Alarm-Collector auf dem EM, DM oder einem eigenständigen Rechner, der eine Verbindung mit der Manager-MDB auf dem DM/EM herstellt. Sie können die Installation auch auf einem eigenständigen Rechner in der Rolle *Alarme weiterleiten* durchführen.

Im folgenden Abschnitt werden die Rollen erläutert, die Sie basierend auf den Konfigurationen auswählen können:

Für den Enterprise-Manager oder einen eigenständigen Server, der eine Verbindung mit dem EM herstellt

Wählen Sie *Alarme in der MDB beibehalten* aus. Für EM werden die anderen Rollen nicht unterstützt.

Für den Domain Manager oder einen eigenständigen Server, der eine Verbindung mit dem DM herstellt

Wählen Sie *Alarme in der MDB beibehalten und konfigurierte Aktionen ausführen* oder *Alarme in der MDB beibehalten, konfigurierte Aktionen ausführen und sie weiterleiten* aus. Wählen Sie letztere Option aus, wenn der Domänen-Manager mit einem Enterprise-Manager verbunden ist, um Alarme an den Enterprise-Manager weiterzuleiten. Wählen Sie andere Rollen aus, wenn Sie nur Alarme in der MDB beibehalten oder einen Alarm-Collector an den Enterprise-Manager weiterleiten möchten.

Eigenständiger Server – der keine Verbindung mit dem DM oder EM herstellt

Wählen Sie *Alarme weiterleiten* aus, um Alarme an einen anderen Alarm-Collector weiterzuleiten. Installieren Sie zum Beispiel in einer ENC-Umgebung den Alarm-Collector auf dem ENC-Server, der sich in der DMZ befindet, damit die Alarme an den Alarm-Collector auf dem DM weitergeleitet werden.

Standardmäßig können Sie den Alarm-Collector direkt auf den Domänen- oder Enterprise-Manager (sofern vorhanden) oder separaten Servercomputern installieren, die mit den MDBs über die Manager verbunden sind. Führen Sie folgende Schritte aus, um die zunehmende Auslastung handzuhaben:

- Fügen Sie zusätzliche Alarm-Collector-Server hinzu, wobei jeder an den Alarm-Collector auf dem Domänen-Manager umgeleitet wird.
- Erhöhen Sie die Anzahl an Worker-Prozessen für den Anwendungspool "DSM_WebService_HM" unter IIS.

Einschränkungen für Computer-, Benutzer- und Verzeichnisnamen

Computer-, Benutzer- und Verzeichnisnamen müssen für das Betriebssystem gültig sein, unter dem CA ITCM installiert wird. Ferner müssen sie folgende Anforderungen erfüllen:

- Einschränkungen für Computernamen (siehe Seite 162)
- Einschränkungen für Benutzernamen (siehe Seite 163)
- Einschränkungen für Verzeichnisnamen (siehe Seite 163)

Einschränkungen für Computernamen

Computernamen dürfen nur die folgenden ASCII-Zeichen enthalten:

- alphanumerische Zeichen
- Bindestriche -

Computernamen dürfen nicht mit einem Bindestrich beginnen.

Wichtig! Es ist erforderlich, dass die zugrunde liegende Domänennamen-System-Infrastruktur (DNS) die UTF-8-Zeichenkodierung in DNS unterstützt, um lokalisierte Hostnamen, d. h. Hostnamen in anderen Sprachen als Englisch, zu unterstützen.

Einschränkungen für Benutzernamen

Benutzernamen dürfen nur die folgenden ASCII-Zeichen enthalten:

- alphanumerische Zeichen
- At-Zeichen @
- Nummernzeichen #
- Dollar $
- Unterstriche _

Benutzernamen dürfen nicht mit @, #, $ oder einer Ziffer beginnen.

Einschränkungen für Verzeichnisnamen

Ein Verzeichnisname muss mit einem der folgenden Zeichen beginnen:

- einem ASCII-Buchstaben (d. h. a-z und A-Z)
- einer Ziffer zwischen 0 und 9
- einem Unterstrich _

Er kann mit den folgenden Zeichen fortgesetzt werden:

- ASCII-Buchstaben
- Ziffern
- Bindestriche -
- Unterstriche _
- Punkt .
- Tilde ~

CA Technologies empfiehlt im Allgemeinen, Pfadnamen nicht durch Groß- und Kleinschreibung zu unterscheiden.

Besondere Hinweis zu Windows:

- Absolute Verzeichnisnamen müssen mit einer Laufwerkangabe beginnen (d. h. mit einem Laufwerksbuchstaben, auf den ein Doppelpunkt folgt). Darauf folgt ein umgekehrter Schrägstrich \, auf den wiederum ein relativer Verzeichnispfad folgt. UNC-Pfade sind nicht zulässig.
- Runde Klammern (und) können nach dem ersten Zeichen eines Verzeichnisnamens verwendet werden. Wenn jedoch ein Manager installiert wird, sind runde Klammern (und) und der Bindestrich - im Verzeichnisnamen nicht zulässig.
- Leerzeichen sind nach dem ersten Zeichen eines Verzeichnisnamens zulässig.
- Es wird nicht zwischen Großbuchstaben und Kleinbuchstaben unterschieden (z. B. ist "A" identisch mit "a").
- Unter Windows ist es nicht möglich, einen DSM-Manager mit einer lokalen MDB oder einer Remote-MDB unter Verwendung eines UNC-Pfades für den Image-Speicherort zu installieren. Wenn sich der Image-Speicherort auf einem Remote-System befindet, muss der Zugriff darauf als Windows-Freigabe hergestellt werden. Der Pfad darf auch kein @ enthalten.

Besondere Hinweise zu Linux und UNIX:

- Absolute Verzeichnispfade müssen mit einem Schrägstrich (/) beginnen und mit einem relativen Verzeichnispfad fortgesetzt werden. Ein relativer Verzeichnispfad enthält mehrere Verzeichnisnamen, die mit Schrägstrichen getrennt sind.
- Es wird zwischen Großbuchstaben und Kleinbuchstaben unterschieden (z. B. ist "A" nicht identisch mit "a").
- Leerraum (z. B. Leertaste und Tabulatorzeichen) ist in Pfaden von Installationsverzeichnissen nicht zulässig.

Interaktive Installation mit dem Installationsassistenten

Der CA ITCM-Installationsassistent verwaltet die gesamte Installation aller Softwarekomponenten und einiger Voraussetzungen. Wenn einige Voraussetzungen fehlen, meldet der Installer Fehlermeldungen.

Prüfung der Festplatte vor der Installation

Das Setup-Programm schätzt ein, welche Kapazität auf der Festplatte zum Installieren der ausgewählten Komponenten benötigt wird. Die Installation wird nur fortgesetzt, wenn die Kapazität auf der Festplatte ausreicht.

Jedoch sind normalerweise beträchtliche Mengen an zusätzlichem Speicherplatz für die Datenspeicherung erforderlich.

Interaktive Installation einzelner Komponenten

So installieren Sie eine oder mehrere einzelne Komponenten in einer bestehenden CA ITCM-Installation:

1. Führen Sie den Installationsassistenten aus, und wählen Sie die Option "CA ITCM installieren".

   Wenn eine bestehende Installation gefunden wird, wird das Dialogfeld "Installationsoption auswählen" angezeigt.

   Wählen Sie die Option "Installation ändern", und befolgen Sie die Anweisungen im Installationsassistenten.

2. Wählen Sie im Dialogfeld "Komponenten und Funktionen auswählen", in dem alle verfügbaren Funktionen angezeigt werden, die Funktionen aus, die Sie installieren möchten.

   Hinweis: Die bereits installierten Funktionen sind ausgewählt. Wenn Sie die Auswahl einer bestehenden Funktion aufheben, wird diese Funktion entfernt.

3. Befolgen Sie die Anweisungen in den folgenden Dialogfeldern des Installationsassistenten, und geben Sie die erforderlichen Informationen für Installation und Konfiguration ein.

Installationszusammenfassung

Während der Installation erfasst das Installationsprogramm Informationen zu allen Schritten, die nach dem Aufrufen des Setup-Programms ausgeführt wurden. Eine Zusammenfassung der Installation enthält eine Liste der Komponenten, die ein Benutzer für die Installation ausgewählt hat. Die Zusammenfassung wird dem Benutzer vor Anfang der Installation angezeigt.

Unter Windows steht die Installationsübersicht nach Abschluss der Installation auch als Textdatei "DSMSummary.txt" zur Verfügung. Die Textdatei "Installationsübersicht" wird in dem Verzeichnis gespeichert, das mit der Umgebungsvariable "%temp%" angegeben wird.

Unter Linux und UNIX wird die Zusammenfassung der Installation in der Hauptinstallations-Protokolldatei gespeichert. Sie ist standardmäßig:

/opt/CA/installer/log/ca-dsm.install.log.

Rollback der Installation

Wenn die Installation einer der vom Setup-Programm aufgerufenen Komponenten fehlschlägt oder nicht abgeschlossen werden kann, wird ein Rollback für dieses Paket und andere Pakete, die im Rahmen der Installationssitzung installiert wurden, ausgeführt, um einen konsistenten Zustand des Systems wiederherzustellen.

Kopie der Installationspakete

Das Setup-Programm optimiert die Nutzung der Festplattenkapazität, indem nur die Pakete vom Installationsdatenträger (DVD) auf das lokale System oder in die Softwarepaketbibliothek kopiert werden, die auch tatsächlich für die ausgewählte Funktionalität benötigt werden. Denken Sie an die folgenden Fälle:

- Wenn die Funktionalität "Infrastructure Deployment" für die Installation ausgewählt wurde, werden die Installationspakete für Agenten und Server vom Installationsdatenträger in das lokale System kopiert.
- Wenn die Software Delivery-Manager-Funktionalität installiert wird, werden alle Installationspakete, einschließlich DSM-Explorer und -Manager, in den Ordner "AUTOREG" der Softwarepaketbibliothek kopiert.

In diesen Fällen werden nur Pakete, die für die ausgewählte Funktionalität benötigt werden, in das lokale System und die Softwarepaketbibliothek kopiert. Wenn alle Funktionalitäten ausgewählt wurden, werden alle Pakete kopiert. Wenn nur die Software Delivery-Funktionalität ausgewählt wurde, werden nur die für Software Delivery benötigten Pakete kopiert.

Hinweise zu CCS

Das DSM-Manager-Setup wählt automatisch die entsprechende Variante von CA Common Services (CCS) aus, und zwar entweder Micro-CCS oder CCS-Vollversion. Die Anwendung installiert Micro-CCS mit dem DSM-Manager, wenn sich dessen MDB auf Oracle befindet. Die CCS-Vollversion wird zusammen mit einer Microsoft SQL Server-MDB installiert.

Wenn Sie den DSM-Manager aktualisieren, versucht das DSM-Manager-Setup, entweder die CCS-Vollversion oder Micro-CCS entsprechend zu aktualisieren.

Die Option "CCS installieren" ist weiterhin auf der obersten Ebene des CA ITCM-Installationsassistenten verfügbar. Hiermit wird die CCS-Vollversion auf dem lokalen Computer installiert. Für diese Option ist Microsoft SQL Server mit der vorinstallierten MDB erforderlich.

In dieser Version wurde jedoch die Option "CCS einschließlich MDB installieren" aus der obersten Ebene des CA ITCM-Installationsassistenten entfernt.

Interaktive Installation von CA IT Client Manager unter Windows

Wir empfehlen, dass Sie zunächst die Option "Voraussetzungen prüfen" ausführen, um sicherzustellen, dass die entsprechende vorausgesetzte Software vorhanden ist, bevor Sie die Installation starten. Hinweise zu CCS finden Sie hier.

Gehen Sie folgendermaßen vor, um CA ITCM interaktiv zu installieren:

- Melden Sie sich beim System als Administrator an.
- Mounten Sie die Installations-DVD oder führen Sie den Setup-Befehl aus, um den Installationsassistenten zu öffnen.
- Befolgen Sie die Anweisungen des Installationsassistenten, und geben Sie die erforderlichen Informationen für Installation und Konfiguration ein. Der Installationsassistent bietet Ihnen hilfreiche Erklärungen und Hinweise auf den Installationsbildschirmen.
- Das erste Dialogfeld des Installationsassistenten ermöglicht Ihnen die Auswahl der Sprache, die während der Installation verwendet werden soll.

Auf dem Begrüßungsbildschirm zeigt der Installationsassistent folgende Optionen an:

CA ITCM installieren

Hierüber können Sie die Produktfunktionalitäten auswählen, die installiert werden sollen, wenn Sie die Lizenzvereinbarung akzeptiert haben.

Installieren von MDB

Hierüber können Sie die Management-Datenbank (MDB) auf einem dedizierten Host ohne CCS-Komponenten (CA Common Services) installieren. Alle Komponenten, die die MDB benötigen, greifen per Remote-Zugriff darauf zu. Diese Installationsoption verhindert, dass der Manager die CCS-Funktionalität verwendet.

Installieren von CCS

Startet eine interaktive Installation von CCS.

CCS einschließlich MDB installieren

Startet die CCS-Installation einschließlich der Management-Datenbank (MDB). Sie müssen diese Option auswählen, wenn Sie den DSM-Manager gemeinsam mit der CCS-Funktionalität verwenden möchten.

Voraussetzungen überprüfen

Prüft die Hostumgebung und ermittelt, ob die Produktinstallation erfolgreich ausgeführt werden kann. Diese Anwendung informiert sie, wenn externe Voraussetzungen fehlen. Sie müssen die erforderliche Software installieren, bevor die CA ITCM-Installation fortgesetzt werden kann.

Dokumente anzeigen

Bietet eine Liste der Dokumentationsdateien im PDF-Format, die Sie im kostenlosen Acrobat Reader lesen können.

Kontaktinformationen

Die offiziellen Post-, Web- und E-Mail-Adresse von CA Technologies und die Telefon- und Faxnummer des Unternehmens.

Interaktive Installation unter Linux und UNIX

Gehen Sie folgendermaßen vor, um CA IT Client Manager unter Linux und UNIX interaktiv zu installieren:

1. Meldern Sie sich beim Linux- oder UNIX-Computer als Benutzer "Root" an.
2. Mounten Sie die Installations-DVD, wechseln Sie zum Stammverzeichnis der DVD, und führen Sie das Skript aus:
   ```
   # sh ./setup.sh
   ```
   Der Installationsassistent wird gestartet. Stellen Sie sicher, dass Sie über die Angaben zu den Verzeichnissen verfügen, in denen die Komponenten installiert werden.
3. Befolgen Sie die Anweisungen des Installationsassistenten, und geben Sie die erforderlichen Informationen für Installation und Konfiguration ein.

Das erste Dialogfeld ermöglicht Ihnen die Auswahl der Sprache, die während der Installation verwendet werden soll.

Im darauf folgenden Dialogfeld "Willkommen" werden folgende Optionen bereitgestellt:

DSM installieren

Hierüber können Sie die Produktfunktionalitäten auswählen, die installiert werden sollen, wenn Sie die Lizenzvereinbarung akzeptiert haben.

Dokumente anzeigen

Bietet eine Liste der Dokumentationsdateien im PDF-Format, die Sie im kostenlosen Acrobat Reader lesen können.

Kontaktinformationen

Die offiziellen Post-, Web- und E-Mail-Adresse von CA Technologies und die Telefon- und Faxnummer des Unternehmens.

Wenn Sie die Option "DSM installieren" auswählen, führt Sie der Installationsassistent zuerst zum Dialogfeld "Endbenutzer-Lizenzvereinbarung". Nach Annahme des Lizenzvertrags können Sie eine beliebige Kombination der folgenden Funktionalitäten installieren:

- Asset Management
- Remote Control
- Software Delivery

Sie können alle Features und Funktionen installieren, auch wenn Sie noch keine Lizenz für das Produkt erworben haben und die Funktionalität während der Testphase nutzen.

Das darauf folgende Dialogfeld des Installationsassistenten fordert Sie zur Auswahl der Installationsmethode auf.

Hinweis: Bei dem Installationsassistent unter UNIX und Linux handelt es sich standardmäßig um eine grafische Java-Benutzeroberfläche (GUI). Wenn es nicht möglich ist, eine grafische Benutzeroberfläche anzuzeigen, z. B., wenn die Installation über eine zeichengestützte Konsole erfolgt, können Sie die Benutzeroberfläche im VT100-Stil (zeichengestützt) des Installationsassistenten verwenden.

Installation von CA ITCM über die Befehlszeile in Windows

In den folgenden Abschnitten werden Informationen zu Tools, Installationspaketen und Installationsoptionen dargestellt, mit denen Sie die CA ITCM-Installation unter Windows über die Befehlszeile ausführen und steuern können.

Installationspakete für Windows

Das CA IT Client Manager-Produkt ist in MSI-Pakete gegliedert, um eine effiziente Verteilung im Netzwerk und Installation sicherzustellen und den Netzwerkverkehr für die Agentenbereitstellung zu verringern.

Master-Setup enthält alle Dialogfelder des Installationsprogramms, ermittelt die zum Aufrufen anderer Pakete im Hintergrundmodus erforderlichen Pakete und verwaltet bei Bedarf das Rollback. Alle anderen Pakete installieren die Dateien und Ressourcen, die für die spezifische Komponente benötigt werden.

Drittanbieterprodukte, die intern für DSM-Komponenten vorausgesetzt werden, werden automatisch aus gesonderten MSI-Paketen installiert.

Die MSI-Installationspakete werden auf dem Installationsdatenträger an folgendem Speicherort abgelegt (hierbei steht *Komponente* für Manager, Explorer usw.

`...\WindowsProductFiles_x86\`*`Komponente`*

Installationspakete für Windows

Die folgende Tabelle enthält eine Übersicht der für CA IT Client Manager verfügbaren Installationspakete, ihrer Dateinamen und der in der Windows-Systemsteuerung im Windows-Applet "Software" angezeigten Namen.

Die Installationspakete finden Sie im Ordner "WindowsProductFiles_x86" auf der CA IT Client Manager-Installations-DVD.

Paket	Dateiname	Name in der Windows-Liste "Software"
Master-Setup	setup.exe	CA IT Client Manager
Explorer	Explorer.msi	CA DSM-Explorer
Manager	Manager.msi	CA DSM Manager
Server	Server.msi	CA DSM-Scalability-Server
Basis-Agent	AgtBHW.msi	CA DSM-Agent + Basisinventar-Plug-in
AM Agent	AgtAM.msi	CA DSM-Agent + Asset Management-Plug-in
DTS-Agent	AgtDTS.msi	CA DSM Agent + Data Transport Plug-in
RC Agent	AgtRC.msi	CA DSM-Agent + Remote Control-Plug-in
SD Agent	AgtSD.msi	CA DSM-Agent + Software Delivery-Plug-in
Dokumentation	Documentation.msi	CA DSM-Dokumentation
DMPrimer	dmsetup.exe	CA DSM DMPrimer
ENC-Server	ServerENC.msi	CA ENC-Server
RVI	RVI.msi	CA-DSM-Remote-Virtualisierungsinventar

Installationspakete von Drittanbietern

Die folgende Tabelle enthält eine Übersicht der Installationspakete von Drittanbietern, die für bestimmte DSM-Komponenten erforderlich sind, ihre Dateinamen und ihre Verwendungszwecke. Informationen über Drittanbieter-Produktversionen und -releases finden Sie im Thema zu den verfügbaren TPLAs im CA ITCM-Bookshelf.

Paket	Dateiname	Beschreibung
AMS 12.8	setupwin32.exe	CA Technologies-Komponente für Asset Maintenance System. Erforderlich für Webdienste.
CCS r11.2	setup.exe	CA Technologies-Komponente für CA Common Services. Erforderlich für Manager-Installationen.

Paket	Dateiname	Beschreibung
AMS 12.8	setupwin32.exe	CA Technologies-Komponente für Asset Maintenance System. Erforderlich für Webdienste.
MDAC	mdac_typ.exe	Microsoft Data Access-Paket. Erforderlich für den Manager-Datenbankzugriff.
Apache Tomcat 7.0.40		Apache Tomcat-Installation. Erforderlich für die Webkonsole.
CA SSA 3.2.0	CA Secure Socket Adapter_NoEtpki.msi	CA Secure Socket Adapter.
CAPKI 4.3.0	Setup.exe	CA PKI-Bibliotheken

Installation von CA IT Client Manager mit Hilfe von "setup.exe"

Starten Sie die Installation oder Konfiguration von CA IT Client Manager über die Befehlszeile, indem Sie im Verzeichnis "WindowsProductFiles_x86" des Installationsdatenträgers die Datei "setup.exe" ausführen.

Sie können beim Ausführen des Programms "setup.exe" die folgenden Optionen einstellen:

/a

Startet eine administrative Installation, die alle DSM-Komponenten und -Dateien in eine Netzwerkfreigabe dekomprimiert.

Hinweis: Dieser Parameter funktioniert nur, wenn sich die Datei "setup.exe" im Produktdateiverzeichnis befindet, und nicht, wenn sie sich im Stammverzeichnis des Installationsdatenträgers befindet.

/V"/l*v x:\DSMSetupxxx.log"

Legt den Pfad der Protokolldatei fest. Protokolldateinamen sind statisch, d. h,. sie können nicht verändert werden.

Installationstool msiexec

Die MSI-Installationspakete unterstützen eine Befehlszeilenschnittstelle. Diese kann beim Bereitstellen der DSM-Funktionalität auf Remote-Systemen über alternative Methoden, z. B. spezifisch erstellte DVDs oder CDs, oder beim Erstellen CA ITCM-Funktionalität in Hostbereitstellungsimages verwendet werden.

Der Microsoft Windows Installer (MSI) installiert Softwarepakete aus Paketdateien mit der Dateierweiterung "msi".

"Msiexec.exe" ist der ausführbare Befehl, mit dem MSI-Pakete über die Befehlszeile installiert werden können. Msiexec ist ein sehr flexibles Tool mit zahlreichen Befehlszeilenoptionen. Detaillierte Beschreibungen der Optionen und Parameter von msiexec finden Sie in der Microsoft-Online-Hilfe.

Alle MSI-Pakete unterstützen allgemeine Optionen. Außerdem unterstützen einige MSI-Pakete paketspezifische Optionen. Beide Optionsarten können verwendet werden, um genau zu steuern, wie eine bestimmte Anwendung installiert wird.

Im Folgenden finden Sie ein Beispiel für einen msiexec-Befehl, der allgemeine Optionen (/i, -l*v, /qn) und die paketspezifische Manager-Installationsoption ADDLOCAL verwendet:

```
msiexec /i "x:\WindowsProductFiles_x86\Manager\Manager.msi" -l*v
"c:\DSMSetupMgr.log" ADDLOCAL=Manager,MgrDC,MgrAM ALLUSERS=1 /qn
```

Die allgemeinen Optionen und paketspezifischen Optionen werden unter "Allgemeine Optionen für msiexec (siehe Seite 174)" und "Paketspezifische MSI-Eigenschaften (siehe Seite 176)" beschrieben.

Hinweis: Die für das Agentenpaket spezifischen Optionen sind die Installationsparameter, die während der interaktiven Bereitstellung verwendet wurden, um auf der Seite "Agentenkonfiguration" des Bereitstellungsassistenten die zusätzlichen Windows-Installationsoptionen anzugeben. Auf dieser Seite können Sie mehrere Installationsoptionen durch Leerzeichen getrennt eingeben, um bestehende Optionen außer Kraft zu setzen.

Wichtig! Wenn Sie DSM-Komponenten direkt über die MSI-Befehlszeile "msiexec" installieren, sollten Sie die MSI-Installationseigenschaft ALLUSERS immer auf den Wert "1" einstellen (Installation für alle Benutzer, aber der Benutzer benötigt Administratorzugriffsrechte auf dem Computer). Dies ermöglicht eine spätere Aktualisierung, Deinstallation oder Neuinstallation über Software Delivery oder über die Bereitstellungsfunktion eines DSM-Managers. Wenn Sie den Parameter nicht auf diesen Wert einstellen oder ihn nicht angeben, wird die Komponente für den Benutzer registriert, der sie zum ersten Mal installiert. Die Komponente kann anschließend nicht mit Hilfe von Manager-Funktionen verwaltet werden.

Hinweis zum Angeben von Systemnamen:

Wenn der CA ITCM-Installer zur Eingabe eines Systemnamens auffordert, wird Ihnen dringend empfohlen, einen vollständig qualifizierten Domänennamen (FQDN) einschließlich Domänensuffix einzugeben, so dass Computersysteme in anderen Netzwerkdomänen erreichbar sind, auch wenn die Anforderungsweiterleitung nicht für alle beteiligten DNS konfiguriert ist.

Allgemeine Optionen für msiexec

Alle MSI-Pakete unterstützen folgende allgemeine Optionen:

/i ***MSI-Installationspaket***

Installiert oder konfiguriert CA ITCM.

/q n|b|r|f|+|–

Legt die Ebene der Benutzeroberfläche fest.

Option (Kombination)	Ebene der Benutzeroberfläche
q	Keine Benutzeroberfläche.
qn	Keine Benutzeroberfläche.
qb	Elementare Benutzeroberfläche. Verwenden Sie "qb!", um die Schaltfläche "Abbrechen" auszublenden.
qr	Reduzierte Benutzeroberfläche ohne modales Dialogfeld am Ende der Installation.
qf	Vollständige Benutzeroberfläche und modale Dialogfelder für schwerwiegenden Fehler, Beendigung durch Benutzer und Beendigung am Ende der Installation.
qn+	Keine Benutzeroberfläche außer einem modalen Dialogfeld am Ende der Installation.
qb+	Elementare Benutzeroberfläche, bei der ein modales Dialogfeld am Ende der Installation angezeigt wird. Das modale Dialogfeld wird nicht angezeigt, wenn der Benutzer die Installation abbricht. Verwenden Sie "qb+!" oder "qb!+", um die Schaltfläche "Abbrechen" auszublenden.
qb–	Elementare Benutzeroberfläche, ohne modales Dialogfeld. Beachten Sie, dass "/qb+-" keine unterstützte Benutzeroberflächenebene ist. Verwenden Sie "qb-!", oder "qb!-", um die Schaltfläche "Abbrechen" auszublenden.

Hinweis: Die Option "!" ist in Microsoft Windows Installer 2.0 verfügbar und funktioniert nur in einer elementaren Benutzeroberfläche. In einer vollständigen Benutzeroberfläche ist sie nicht gültig.

/l [i|w|e|a|r|u|c|m|o|p|v|x|+|!|*] *Protokolldatei*

Die Protokollierungsinformationen werden in eine Protokolldatei unter dem angegebenen Pfad geschrieben. Flags zeigen an, welche Informationen protokolliert werden. Wenn keine Flags spezifiziert sind, ist die Standardeinstellung "iwearmo".

Flag	Zu protokollierende Informationen
i	Statusmeldungen
w	Nicht schwerwiegende Warnungen
e	Alle Fehlermeldungen
a	Start von Aktionen
o	Aktionsspezifische Datensätze
u	Benutzeranforderungen
c	Anfangsparameter für die Benutzeroberfläche
m	Information über unzureichenden Speicher oder schwerwiegende Abbrüche
o	Meldungen zu fehlendem Speicherplatz
p	Eigenschaften des Terminals
v	Detaillierte Ausgabe
x	Zusätzliche Debugging-Informationen. Nur auf Windows Server 2003 verfügbar
+	An vorhandene Datei anhängen
!	Jede Zeile in das Protokoll schreiben.
*	Platzhalter. Alle Daten außer den Optionen "v" und "x" protokollieren. Um die Optionen "v" und "x" einzuschließen, geben Sie "/l*vx" an.

Paketspezifische MSI-Eigenschaften

Die MSI-Installationspakete für die folgenden DSM-Komponenten und -Plug-in unterstützen paketspezifische Installationseigenschaften:

- DSM-Explorer
- Basisinventar-Agent
- Asset Management-Agent
- Data Transport Service-Agent
- Remote Control-Agent
- Software Delivery-Agent
- Scalability-Server
- Manager
- ENC-Gateway-Server

Hinweis: Sie müssen die paketspezifischen MSI-Eigenschaften als Benutzerparameter an Ihren Software-Job weitergeben. Weitere Informationen zu Benutzerparametern finden Sie im Abschnitt "Software Delivery" der *DSM Explorer-Hilfe* im Thema zur Registerkarte "Jobs".

Voraussetzungen für die Installation von MSI-Paketen

Sie müssen die ETPKI-Bibliotheken und CA Secure Socket Adapter installieren, bevor Sie MSI-Pakete installieren. Die erforderlichen Versionen der vorausgesetzten Software finden Sie im Abschnitt "Installationspakete von Drittanbietern (siehe Seite 171)". Sie müssen Systems Performance LiteAgent installieren, bevor Sie das Asset Management MSI-Paket installieren.

- **Installieren der CAPKI-Bibliotheken:**

  Das Setup für CAPKI finden Sie auf dem CA ITCM-Installationsdatenträger (CD/DVD) im Verzeichnis "WindowsProductFiles_x86\CAPKI".

  Verwenden Sie folgende Befehlszeile, um die CAPKI-Bibliotheken zu installieren:

  ```
  "setup install caller=CADSMCAPKI"
  ```

- **Installieren von CA Secure Socket Adapter:**

  CA Secure Socket Adapter kann mit Hilfe des Secure Socket Adapter-Installationsprogramms auf dem CA IT Client Manager-Installationsdatenträger (CD/DVD) im Verzeichnis "WindowsProductFiles_x86\ETPKI" installiert werden.

  Verwenden Sie folgende Befehlszeile, um CA Secure Socket Adapter zu installieren:

  ```
  msiexec.exe
  /i"D:\WindowsProductFiles_x86\SSA\CASockAdapterSetupWin32NoEtpki.msi" /l*v
  "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DSMSetupSSA.log" /qb-!
  ```

- **Installieren von Systems Performance LiteAgent:**

  Systems Performance LiteAgent kann mit Hilfe des Systems Performance LiteAgent-Installationsprogramms installiert werden, das sich im Verzeichnis "WindowsProductFiles_x86\PMLA" auf dem CA ITCM-Installationsdatenträger (CD/DVD) befindet. Der Systems Performance LiteAgent-DSM-Client muss auch installiert werden.

  Verwenden Sie folgende Befehlszeile, um Systems Performance LiteAgent zu installieren:

  ```
  msiexec.exe /i"D:\WindowsProductFiles_x86\PMLA\CA_SysPerf_LiteAgent.msi" /l*v
  "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DSMSetupPMLiteAgent.log" /qb-!
  ```

  Verwenden Sie folgende Befehlszeile, um den Systems Performance LiteAgent-DSM-Client zu installieren:

  ```
  msiexec.exe
  /i"<Netzlaufwerk>\WindowsProductFiles_x86\PMLA_Client\CA_SysPerf_LiteAgent_UA
  M.msi" /l*v
  "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DSMSetupPMLiteAgentClient.log" /qb-!
  ```

MSI-Eigenschaften für das Explorer-Paket

Das MSI-Installationspaket für den DSM-Explorer (Explorer.msi) unterstützt folgende paketspezifische Eigenschaften:

ADDLOCAL

Spezifische Funktionen, die zur Installation ausgewählt werden können.

Wert	Beschreibung
Explorer	Allgemeine Explorer-Komponenten (für Explorer-Installation obligatorisch)
ExpAM	Asset Management-Plug-in
ExpRC	Allgemeines Remote Control-Plug-in
ExpSD	Allgemeines Software Delivery-Plug-in
ExpSDB	Boot Manager-Plug-in
ExpSDM	Software Delivery Manager-Client-API
ExpRP	Reporter-Plug-in
ALLE	Wählt alle oben genannten Funktionen aus.

ADMINCONSOLE_MANAGER

Managersystem, mit dem der DSM-Explorer eine Verbindung herstellen soll.

Wert: Systemname oder IP-Adresse

MSI-Eigenschaften für das Basisinventar-Agentenpaket

Das MSI-Installationspaket für das Basisinventar-Agenten-Plug-in (AgtBHW.msi) und ENC-Client unterstützen folgende paketspezifische Eigenschaften:

AGENT_SERVER

Scalability-Server, mit dem der Agent eine Verbindung herstellen soll.

Wert: Systemname oder IP-Adresse

AGENT_DEFAULTGROUPS

Eine Gruppe oder eine Liste von Managementgruppen, die im Manager erstellt werden, in dem sich der Agent automatisch registriert.

Wert: Eine durch Kommata getrennte Liste mit Gruppennamen.

Beispiel: Grp1/subgroup1,Group2,...

ENC_CLIENT_ENABLED

Gibt an, ob der ENC-Client aktiviert werden soll, wenn das Basis-Hardware-Inventar installiert wird. Standardmäßig werden die Client-Dateien auf den Computer kopiert, aber nicht ausgeführt. Dies vereinfacht das Installationsprogramm und ermöglicht einem einfachen Konfigurationsjob, den Client bei Bedarf zu einem späteren Zeitpunkt zu aktivieren.

Wert: 0 (Inaktiv lassen), 1 (Aktivieren)

Hinweis: Die folgenden Parameter müssen *nicht* angegeben werden, wenn der ENC-Client nicht aktiviert wird.

ENC_SVR_ADDR

Der ENC-Gateway-Server, zu dem dieser Client eine Verbindung aufbauen soll.

Wert: FQN des Servers

ENC_SVR_TCP_PORT

TCP-Port des ENC-Gateway-Servers, zu dem eine Verbindung hergestellt werden soll.

Standard: 443

ENC_SVR_HTTP_PORT

HTTP-Port des ENC-Gateway-Servers, mit dem eine Verbindung hergestellt werden soll.

Standard: 80

ENC_HTTP_PROXY_ADDR

Adresse des HTTP-Internet-Proxy-Servers, zu dem der ENC-Client eine Verbindung aufbauen muss, um eine Verbindung außerhalb des lokalen Netzwerks herzustellen.

ENC_HTTP_PROXY_PORT

Port-Nummer des Proxys, mit dem verbunden werden soll.

Standard: 8080

ENC_PROXY_ORDER

Die Verbindungstypen, die vom ENC-Client ausprobiert werden sollen. Wenn keine Angabe erfolgt, wird eine Standardreihenfolge verwendet.

Wert: Dies ist eine durch Leerzeichen getrennte Liste aus keinem oder mehreren der folgenden Schlüsselwörter: "socket", "socks4Anon", "socks5Auth", "socks5Anon", "httpConnect", "http" und "httpProxy".

ENC_SOCKS_ADDR

Adresse des SOCKS-Internet-Proxy-Servers, zu dem der ENC-Client eine Verbindung aufbauen muss, um eine Verbindung außerhalb des lokalen Netzwerks herzustellen.

Wert: FQN oder IP-Adresse des Servers

ENC_SOCKS_PORT

Port-Nummer des Proxys, mit dem verbunden werden soll.

Standard: 1080

ENC_SOCKS_USER

Gibt den Benutzernamen an, der beim Verbinden mit einem SOCKS-Server authentifiziert werden soll.

Beispiel: "socksuser"

ENC_SOCKS_PW

Das über "ENC_SOCKS_USER" angegebene Kennwort des Benutzers in Klartext.

ENC_HTTP_PROXY_USER

Gibt den Benutzernamen an, der beim Verbinden mit einem HTTP-Server authentifiziert verwendet werden soll.

Beispiel: "httpuser"

ENC_HTTP_PROXY_PW

Das über "ENC_HTTP_PROXY_USER" angegebene Kennwort des Benutzers in Klartext.

Hinweis: Weitere Informationen zu ENC-Eigenschaften finden Sie in der *encUtilCmd-Befehlsreferenz*. Weitere Informationen hierzu finden Sie auch unter dem Thema "Richtliniengruppe ENC-Gateway" im Abschnitt "Konfigurationsrichtlinie" in der *DSM-Explorer-Hilfe*.

MSI-Eigenschaften für das Asset Management-Agentenpaket

Das MSI-Installationspaket für das Asset Management-Agenten-Plug-in (AgtAM.msi) unterstützt folgende paketspezifische Eigenschaften:

AGENT_SERVER

Scalability-Server, mit dem der Agent eine Verbindung herstellen soll.

Wert: Systemname oder IP-Adresse

AGENT_DEFAULTGROUPS

Eine Gruppe oder eine Liste von Managementgruppen, die im Manager erstellt werden, in dem sich der Agent automatisch registriert.

Wert: Eine durch Kommata getrennte Liste mit Gruppennamen.

Beispiel: Grp1/subgroup1,Group2,...

MSI-Eigenschaften für das Data Transport Service-Agentenpaket

Das MSI-Installationspaket für das Data Transport Service-(DTS-)Agenten-Plug-in (AgtDTS.msi) unterstützt folgende paketspezifische Eigenschaften:

SC_DSMPROP

Verknüpfung zum Dialogfeld "Agenteneigenschaft"

Wert	Beschreibung
1	In das Menü "Start" wird das Dialogfeld "Agenteneigenschaft" eingefügt.
0	Es wird keine Verknüpfung erstellt.

ADDLOCAL

Spezifische Funktionen, die zur Installation ausgewählt werden können.

Wert	Beschreibung
Agent	Allgemeine Agententeile (obligatorisch für Installationen des Agenten)
AgtDTS	Allgemeine Teile des Transport Service-Agenten (obligatorisch für die Installation des DTS-Agenten)
ALLE	Wählt alle oben genannten Funktionen aus.

AGENT_DEFAULTGROUPS

Eine Gruppe oder eine Liste von Managementgruppen, die im Manager erstellt werden, in dem sich der Agent automatisch registriert.

Wert: Eine durch Kommata getrennte Liste mit Gruppennamen.

Beispiel: Grp1/subgroup1,Group2,...

MSI-Eigenschaften für das Remote Control-Agentenpaket

Das MSI-Installationspaket für das Remote Control-Agenten-Plug-in (AgtRC.msi) unterstützt folgende paketspezifische Eigenschaften:

SC_DSMPROP

Verknüpfung zum Dialogfeld "Agenteneigenschaft"

Wert	Beschreibung
1	In das Menü "Start" wird das Dialogfeld "Agenteneigenschaft" eingefügt.
0	Es wird keine Verknüpfung erstellt.

ADDLOCAL

Spezifische Funktionen, die zur Installation ausgewählt werden können.

Wert	Beschreibung
Agent	Allgemeine Agententeile (obligatorisch für Installationen des Agenten)

Wert	Beschreibung
AgtRC	Allgemeine Teile des Remote Control-Agenten (obligatorisch für die Installation des Remote Control-Agenten)
AgtRCA	Remote Control-Host
AgtRCV	Remote Control-Viewer
AgtRCP	Remote Control-Replayer
ALLE	Wählt alle oben genannten Funktionen aus.

AGENT_SERVER

Scalability-Server, mit dem der Agent eine Verbindung herstellen soll.

Wert: Systemname oder IP-Adresse

RC_AGENT_STANDALONE

Wert	Beschreibung
0	Der Remote Control-Agent wird zentral verwaltet.
1	Der Remote Control-Agent ist eigenständig.

AGENT_DEFAULTGROUPS

Eine Gruppe oder eine Liste von Managementgruppen, die im Manager erstellt werden, in dem sich der Agent automatisch registriert.

Wert: Eine durch Kommata getrennte Liste mit Gruppennamen.

Beispiel: Grp1/subgroup1,Group2,...

MSI-Eigenschaften für das Software Delivery-Agentenpaket

Das MSI-Installationspaket für den Software Delivery-Agenten-Plug-in (AgtSD.msi) unterstützt folgende paketspezifische Eigenschaften:

SC_DSMPROP

Verknüpfung zum Dialogfeld "Agenteneigenschaft"

Wert	Beschreibung
1	In das Menü "Start" wird das Dialogfeld "Agenteneigenschaft" eingefügt.

Wert	Beschreibung
0	Es wird keine Verknüpfung erstellt.

ADDLOCAL

Spezifische Funktionen, die zur Installation ausgewählt werden können.

Wert	Beschreibung
Agent	Allgemeine Agentenkomponenten (obligatorisch für Installationen des Agenten)
AgtSD	Allgemeine Komponenten des Software Delivery-Agenten (obligatorisch für die Installation des Software Delivery-Agenten)
AgtSDA	Software Delivery-Komponenten (obligatorisch für den SD-Katalog)
AgtSDC	Software Delivery-Katalog-Komponenten
ALLE	Wählt alle oben genannten Funktionen aus.

AGENT_SERVER

Scalability-Server, mit dem der Agent eine Verbindung herstellen soll.

Wert: Systemname oder IP-Adresse

AGENT_DEFAULTGROUPS

Eine Gruppe oder eine Liste von Managementgruppen, die im Manager erstellt werden, in dem sich der Agent automatisch registriert.

Wert: Eine durch Kommata getrennte Liste mit Gruppennamen.

Beispiel: Grp1/subgroup1,Group2,...

MSI-Eigenschaften für das Scalability-Server-Paket

Das MSI-Installationspaket für Scalability-Server (Server.msi) unterstützt folgende paketspezifische Eigenschaften:

FIPS_MODE

Definiert den vom CA ITCM-Installationsprogramm festgelegten FIPS-Modus.

Wert	Beschreibung
1	FIPS-bevorzugt

Wert	Beschreibung
2	Nur-FIPS

ADDLOCAL

Spezifische Funktionen, die zur Installation ausgewählt werden können.

Wert	Beschreibung
Server	Allgemeine Komponenten des Scalability-Servers (obligatorisch für Serverinstallationen)
SrvAM	Asset Management-Scalability-Server-Plug-in
SrvSD	Software Delivery-Scalability-Server-Plug-in
SrvRC	Remote Control-Scalability-Server-Plug-in
ALLE	Wählt alle oben genannten Funktionen aus.

SRV_SDBPATH

Verzeichnispfad, in dem die Datenbank des Scalability-Servers installiert werden soll.

SERVER_PATH

Verzeichnispfad, in dem die serverspezifischen Daten des Scalability-Servers installiert werden sollen.

SERVER_MANAGER

Managersystem, zu dem der Scalability-Server eine Verbindung herstellen soll.

Wert: Systemname oder IP-Adresse

SERVER_ENGINE

Engine-System, mit dem der Scalability-Server eine Verbindung herstellen soll. Wurde dieser Parameter nicht festgelegt, wird standardmäßig die System-Engine verwendet.

Wert: Engine-Name

BS_OS_PATH

Verzeichnispfad, in dem die BS-Images und andere spezifische Daten des Boot-Servers gespeichert werden. Der Pfad muss mit der Zeichenfolge "\SDBS\var" enden.

Beispiel: f:\Programme\CA\DSM\Server\SDBS\var

CREATESDMSISHARE

Freigabe zum Zugriff auf MSI-Pakete, die beim Software Delivery-Manager registriert sind.

Wert	Beschreibung
1	Erstellt eine Freigabe für den Zugriff auf die MSI-Pakete.
0	Erstellt keine SERVER_ENGINE-Freigabe.

CREATESDLIBSHARE

Freigabe zum Zugriff auf Pakete, die bei der Software Delivery-Bibliothek registriert sind.

Wert	Beschreibung
1	Erstellt eine Freigabe für den Zugriff auf die Pakete.
0	Erstellt keine Freigabe.

BOOTSERVER_ENABLED

Ermittelt, ob der Boot-Server-Dienst aktiviert werden soll.

Wert	Beschreibung
0	Boot-Server-Dienst nicht aktivieren.
1	Boot-Server-Dienst aktivieren.

BOOTSERVER_DISABLESHARES

Freigabe zum Zugriff auf Pakete, die beim Boot-Server registriert sind.

Wert	Beschreibung
0	Erstellt eine Freigabe für den Zugriff auf die Pakete.
1	Erstellt keine Freigabe.

MSI-Eigenschaften für das Manager-Paket

Das MSI-Installationspaket für den Manager (Manager.msi) unterstützt folgende paketspezifische Eigenschaften:

ADDLOCAL

Spezifische Funktionen, die zur Installation ausgewählt werden können.

Wert	Beschreibung
Manager	Allgemeine Managerkomponenten (obligatorisch für Managerinstallationen)
MgrInf	Allgemeine Managerinfrastruktur (obligatorisch für Managerinstallationen)
MgrDC	Engine-Plug-in (obligatorisch für Managerinstallationen)
MgrAM	Asset Management-Manager-Plug-in
MgrRC	Allgemeines Remote Control-Manager-Plug-in
MgrSD	Allgemeines Software Delivery-Manager-Plug-in
MgrDTS	Data Transport Service-Manager-Plug-in (obligatorisch für jede Installation von Software Delivery-Manager)
MgrDM	Bereitstellungs-Manager-Plug-in
MgrIP	Image Prepare-Manager-Plug-in
ALLE	Wählt alle oben genannten Funktionen aus.

DMSOFTLIBDIR

Verzeichnispfad, in dem die Pakete für DMDeploy installiert werden sollen.

DMKEYLOCATION

Verzeichnispfad für die Schlüsseldatei des Bereitstellungs-Managers.

SDLIBRARY

Verzeichnispfad, in dem die Softwarepaketbibliothek installiert werden soll.

MANAGER_ROLE

Rolle des Managers.

Wert	Beschreibung
0 = Enterprise	Der Manager agiert als Enterprise-Manager.
1 = Mitglied der Domäne.	Der Manager agiert als Domänen-Manager in einem Enterprise.

Wert	Beschreibung
2 = Eigenständiger Manager	Der Manager agiert als eigenständiger Domänen-Manager.

ENTERPRISE_NAME

Das Enterprise-Manager-System, mit dem der Domänen-Manager eine Verbindung herstellen soll, wenn die Rolle als Domänen-Mitglied (Wert = 1) festgelegt wurde. Anderenfalls ist diese Eigenschaft leer.

Wert: Systemname oder IP-Adresse

WAC_MANAGER

Webkonsolen-Managersystem für eine eigenständige Installation der Webkonsole.

Wert: Systemname oder IP-Adresse

ENGINE_MANAGER

Engine-Manager-System für eine eigenständige Installation der Engine.

Wert: Systemname oder IP-Adresse

DSM_TOMCAT_PORT

TCP/IP-Port, den der Handler auf Anforderungen überwacht.

Standard: 8090

DSM_TOMCAT_SHUT

TCP/IP-Port, den der Handler auf Anforderungen zum Herunterfahren überwacht.

Standard: 8095

DSM_TOMCAT_AJP

Port, den der Worker auf Ajp13-Anforderungen überwacht, um Anforderungen an Out-of-Process-Workers weiterzuleiten, die das Ajpv13-Protokoll verwenden.

Standard: 8020

DB

Typ der verwendeten Datenbank.

Wert: SQLServer oder Oracle

DBSERVER

Name des Systems, in dem sich die Datenbank befindet.

Wert: Systemname oder IP-Adresse

DBUSERNAME

Windows-Benutzername für den Datenbankzugriff

DBPASSWORD

Kennwort für DBUSERNAME.

DBVUSER

Vnode im Datenbanksystem, wenn es sich bei der Datenbank um Ingres handelt und ein Remote-Datenbanksystem verwendet wird.

DBVPWD

Kennwort für DBVUSER.

DBSW

Gibt per Flag an, ob die Softwaresignaturen für die Softwareerkennung in der Management-Datenbank eingefügt (eingeschlossen) sein müssen oder nicht (ausgeschlossen).

Wert	Beschreibung
excl_sw	Keine Softwaresignaturen einfügen.
incl_sw	Softwaresignaturen einfügen.

FAILOVER_ENABLED

Gibt per Flag an, ob die Wiederherstellungsunterstützung aktiviert oder deaktiviert ist.

Wert	Beschreibung
0	Wiederherstellungsunterstützung ist deaktiviert.
1	Wiederherstellungsunterstützung ist aktiviert.

FAILOVER_STATUS

Gibt per Flag an, ob dieser Manager ein aktiver oder ein passiver Knoten in einer Cluster-Umgebung ist.

Wert	Beschreibung
0	Dieser Manager ist ein passiver Manager.
1	Dieser Manager ist der aktive Manager.

FAILOVER_CLUSTER_NAME

Cluster-Name des Managers

MSI-Eigenschaften für das ENC-Gateway-Server-Paket

Das MSI-Installationspaket für den ENC-Gateway-Server unterstützt folgende paketspezifische Eigenschaften:

AGENT_SERVER

Scalability-Server, mit dem der Agent eine Verbindung herstellen soll.

Wert: Systemname oder IP-Adresse

ENC_CLIENT_ENABLED

Gibt an, ob der ENC-Client aktiviert werden soll, wenn der ENC-Gateway-Server installiert wird.

Wert: 0 (Inaktiv lassen), 1 (Aktivieren)

ENC_SERVER_TYPE

Gibt die Rollen für den ENC-Gateway-Server an. Dies sollte mindestens einer der in der folgenden Tabelle aufgelisteten Werte sein. Die Werte müssen durch Leerzeichen getrennt angegeben werden. Ein ENC-Gateway-Server kann eine oder mehrere Rollen einnehmen. Wenn ein Manager angegeben wird, wird automatisch auch ein Server konfiguriert. Der ENC-Client wird auch automatisch zur Registrierung auf dem Server konfiguriert.

Wenn nur ein ENC-Gateway-Server konfiguriert wird, registriert sich der Client auch auf diesem.

In beiden oben genannten Fällen werden die Konfigurationsparameter für den Client nicht benötigt, abgesehen von ENC_CLIENT_ENABLED.

Wenn nur ein Router konfiguriert wurde, müssen sich der Client und der Router bei einem anderen ENC-Gateway-Server anmelden. Stellen Sie hierzu den Parameter ENC_SVR_ADDR ein.

Wert	Beschreibung
ENC_SRS	Zur Verwendung als ENC-Gateway-Registrierungsserver konfigurieren.
ENC_ROUTER	Zur Verwendung als ENC-Gateway-Router konfigurieren.
ENC_MRS	Zur Verwendung als ENC-Gateway-Manager konfigurieren.

ENC_SVR_ADDR

Wenn Sie einen ENC-Gateway-Router installieren, dann sollte dies der ENC-Gateway-Server sein, bei dem die Registrierung durchgeführt wird.

Wenn Sie einen ENC-Gateway-Registrierungsserver installieren, dann sollte dies der ENC-Gateway-Registrierungsmanager sein, mit dem die Registrierung durchgeführt wird.

Wert: FQN des ENC-Gateway-Servers bzw. -Managers, bei dem die Registrierung durchgeführt werden soll.

Hinweis: Wenn Sie einen ENC-Gateway-Manager installieren, dann wird dies automatisch konfiguriert.

ENC_SVR_TCP_PORT

TCP-Port des ENC-Gateway-Managers, mit dem eine Verbindung hergestellt werden soll.

Standard: 443

Hinweis: Wenn Sie einen ENC-Gateway-Manager installieren, dann wird dies automatisch konfiguriert.

ENC_SVR_HTTP_PORT

HTTP-Port des ENC-Gateway-Managers, mit dem der ENC-Gateway-Registrierungsserver oder Router eine Verbindung herstellt.

Standard: 80

Hinweis: Wenn Sie einen ENC-Gateway-Registrierungsmanager installieren, wird dies automatisch konfiguriert. Dies muss nur für Gateway-Server oder -Router festgelegt werden.

Hinweis: Weitere Informationen zu ENC-Eigenschaften finden Sie in der *encUtilCmd-Befehlsreferenz*. Weitere Informationen hierzu finden Sie auch unter dem Thema "Richtliniengruppe ENC-Gateway" im Abschnitt "Konfigurationsrichtlinie" in der *DSM-Explorer-Hilfe*.

Zusätzliche Eigenschaften für msiexec

Die folgenden Eigenschaften gelten für alle von CA Technologies bereitgestellten MSI-Installationspakete:

CA

Installationsverzeichnis auf dem Zielsystem.

Beispiel: C:\Programme\CA

CONFIGDATA_LOCATION

Installationsverzeichnis für die Konfigurationsdaten des Pakets, einschließlich des Konfigurationsspeichers (comstore).

Standard: Produktinstallationsverzeichnis.

Beispiel: C:\Programme\CA\DSM

SHAREDCOMPONENTS

Installationsverzeichnis für die freigegebenen Komponenten des Pakets.

Beispiel: C:\Programme\CA\SC

Hinweis: **Sobald ein Paket installiert wurde, sind die Werte dieser allgemeinen Eigenschaften für alle Pakete festgelegt, die danach installiert werden.**

Für jedes MSI-Installationspaket können Sie zusätzlich folgende Eigenschaften festlegen:

DSM_LANGUAGE

Gibt die Sprache der CA IT Client Manager-Installation an. Mögliche Wert sind: "enu" (Englisch/US), "deu" (Deutsch), "fra" (Französisch) und "jpn" (Japanisch).

Zwar werden die Dateien für alle unterstützten Sprachversionen von CA IT Client Manager installiert, für die tatsächliche Installation wird jedoch die von DSM_LANGUAGE angegebene Sprache verwendet.

Standard: Leer (NULL). Hierdurch verwendet das Installationsprogramm das standardmäßige Gebietsschema des Systems. Wenn das Standardgebietsschema des Systems nicht unterstützt wird, wird für die Installation das Gebietsschema "enu" (Englisch/US) verwendet.

Hinweis: Die Sprache der Dialogfelder der Installationsassistenten wird von DSM_LANGUAGE nicht angegeben.

REBOOT

Wert	Beschreibung
REALLYSUPPRESS	Wenn ein Neustart erforderlich ist, wird er in jedem Fall unterdrückt und muss manuell ausgeführt werden.

ALLUSERS

Wert	Beschreibung
0	Installation für einen einzelnen Benutzer.
1	Installation für alle Benutzer, aber der Benutzer benötigt Administratorzugriffsrechte auf dem Computer.
2	Installation für alle Benutzer, wenn der Benutzer Administratorzugriff hat. Andernfalls erfolgt die Installation für einen einzelnen Benutzer.

Hinweis: Wenn Sie DSM-Komponenten direkt über die MSI-Befehlszeile installieren, müssen Sie immer "ALLUSERS=1" festlegen, um spätere Aktualisierungen, Deinstallationen oder Neuinstallationen über Software Delivery oder über die Bereitstellungsfunktion eines Managers zu ermöglichen. Wenn Sie den Parameter nicht auf diesen Wert einstellen oder ihn nicht angeben, wird die Komponente für den Benutzer registriert, der sie zum ersten Mal installiert. Die Komponente kann anschließend nicht mit Hilfe von Manager-Funktionen verwaltet werden.

ARPSYSTEMCOMPONENT

Wenn Sie die Eigenschaft festlegen, wird die Anwendung nicht in der Liste "Software" der Windows-Systemsteuerung angezeigt. Diese Eigenschaft funktioniert nicht in Versionen von Betriebssystemen vor Windows 2000 und Windows XP.

CAF_INSTALL_SERVICE

Wert	Beschreibung
0 | 1	Muss für das erste auf dem System installierte MSI-Paket "1" sein. Für alle anderen kann der Wert "0" sein.

CAF_START_SERVICE

Wert	Beschreibung
0 | 1	Muss für das letzte auf dem System installierte MSI-Paket "1" sein. Für alle anderen muss der Wert "0" sein.

FIPS_MODE

Wert	Beschreibung
1	Installiert CA ITCM in FIPS-bevorzugter Modus (Standard)
2	Installiert CA ITCM im "Nur-FIPS-"-Modus

Optionen für msiecex zum Deinstallieren, Reparieren und für die Verwaltungsinstallation

Mit der MSI-Befehlszeilenoberfläche können Sie Tasks zum Deinstallieren, Reparieren oder für die Verwaltungsinstallation initiieren:

/x msi_install_package | Produktcode

Deinstalliert ein Produkt.

/f [p|o|e|d|c|a|u|m|s|v] msi_install_package | Produktcode

Repariert ein Produkt. Mit dieser Option werden alle in der Befehlszeile eingegebenen Eigenschaftswerte ignoriert. Die standardmäßige Argumentliste für diese Option ist "omus". Diese Option nutzt die gleiche Argumentliste wie die Eigenschaft REINSTALLMODE.

Option	Beschreibung
p	Nur neu installieren, wenn Datei fehlt.
o	Neu installieren, wenn Datei fehlt oder eine ältere Version installiert ist.
e	Neu installieren, wenn Datei fehlt oder eine gleiche oder ältere Version installiert ist.
d	Neu installieren, wenn Datei fehlt oder eine andere Version installiert ist.
c	Neu installieren, wenn die Datei fehlt oder die gespeicherte Kontrollsumme nicht mit dem berechneten Wert übereinstimmt. Nur Dateien reparieren, in deren Tabelle "Datei" in der Spalte "Attribute" "msidbFileAttributesChecksum" angegeben ist.
a	Neuinstallation aller Dateien erzwingen.
u	Alle erforderlichen Benutzerregistrierungseinträge neu schreiben.
m	Alle erforderlichen computerspezifischen Registrierungseinträge neu schreiben.
s	Überschreibt alle vorhandenen Verknüpfungen.
v	Wird von der Quelle ausgeführt und zwischenspeichert das lokale Paket. Verwenden Sie für die erste Installation einer Anwendung oder Funktion nicht die Neuinstallationsoption "v".

/a msi_install_package

Verwaltungsinstallationsoption. Installiert ein Produkt in einer Netzwerkfreigabe. Von dort aus kann es im Netzwerk installiert werden.

Beispiele für die Kombination der Optionen und Eigenschaften von msiexec.

In den folgenden Beispielen wird dargestellt, wie Sie die Optionen und Eigenschaften von msiexec kombinieren können.

```
msiexec.exe
/i"N:\DSM_11_2_9999_0_DVD\WindowsProductFiles_x86\Manager\Manager.msi"
/l*v "G:\DOCUME~1\KSYST0~1.TAN\LOCALS~1\Temp\DSMSetupManager.log"
ADDLOCAL=Manager,MgrAM,MgrRC,MgrSD,MgrDC,MgrDTS,MgrDM,MgrIP
REBOOT=REALLYSUPPRESS ALLUSERS=1
CA="G:\Programme\CA\DSM\"
CAF_INSTALL_SERVICE="1" CAF_START_SERVICE="0"
/qb-! DMSOFTLIBDIR="G:\Programme\CA\DSM"
SDLIBRARY="G:\Programme\CA\DSM\SD\ASM\LIBRARY"
ENTERPRISE_NAME="KSYST01U"
MANAGER_ROLE="2" DB="SQLServer"
DBSERVER="KSYST01U" DBUSERNAME="ca_itrm" DBPASSWORD=XXX DBSW="excl_sw"
```

Installation von CA ITCM über die Befehlszeile in Linux und UNIX

Sie installieren CA ITCM unter Linux oder UNIX mit dem Skript "installdsm", das Sie im Verteilungsverzeichnis unter "LinuxProductFiles_x86/component" finden.

Hinweis: CADSMCMD wird nur für Linux, nicht jedoch für andere UNIX-Derivate bereitgestellt. Weitere Informationen finden Sie im *<CLI>-Referenzhandbuch*.

Wie bei der Windows-Installation befindet sich im Stammverzeichnis der Installations-DVD eine Skriptdatei namens "setup.sh". Dieses Skript ruft "/LinuxProductFiles_x86/manager/installdsm" auf.

Der Installer für Linux und UNIX wird standardmäßig im interaktiven Modus ausgeführt. Wenn CA ITCM bereits auf dem System installiert ist, bietet der Installer die Option zum Aktualisieren/Reparieren, Ändern oder Deinstallieren.

Der Installationsdatenträger enthält auch eine Antwortdatei-Vorlage: "install.rsp". Mit Hilfe dieser Datei können unbeaufsichtigte Installationen erstellt werden.

Skript "installdsm" - Installation von CA ITCM unter Linux oder UNIX

Das Skript "installdsm" hat folgendes Format:

```
installdsm [-f | -r Antwortdatei [/Rname=Wert…] | -g Antwortdatei ]
```

-f

Erzwingt die Installation ohne Sicherungskopie von bestehenden älteren Produktversionen.

-r *Antwortdatei* [/R*Name*=*Wert* ...]

Führt mit den in der Antwortdatei angegebenen Werten eine unbeaufsichtigte Installation aus. Wenn Sie die Option "-r" angeben, prüft "installdsm", dass die Antwortdatei nicht leer ist und gültige Bezeichnungswertpaare enthält. Die Angabe "/R" setzt die in der Antwortdatei angegebenen Parameter außer Kraft. Geben Sie für jeden Parameter, der außer Kraft gesetzt werden soll, die Option "/R" an, beispielsweise:

```
installdsm -r rsp.txt \
/RITRM_AUTOSTART_INSTALL=1 \
/RITRM_AUTOSTART_REBOOT=1
```

Es wird nicht geprüft, ob die Namen oder Werte der Parameter gültig sind oder ob sich die genannten Parameter in der Antwortdatei befinden.

Alle Linux- und UNIX-Pakete enthalten eine Beispielantwortdatei namens "install.rsp" mit einer Liste der Standardparametereinstellungen.

Wenn Sie das Installationsprogramm für eine interaktive Installation oder zum Erstellen einer Antwortdatei für eine unbeaufsichtigte Installation verwenden, müssen Sie jedes Mal die Parameterwerte bearbeiten. Wenn das Installationsskript Sie zum Eingeben der Optionen aufgefordert hat, kopiert das Installationsprogramm die Dateien und führt die Konfigurationsaktionen aus.

-g *Antwortdatei*

Erzeugt eine Antwortdatei. Das Skript zeigt die Dialogfelder wie bei einer interaktiven Installation an, aber am Ende der Dialogabfolge werden alle angegebenen Eigenschaftswerte in die angegebene Antwortdatei geschrieben.

Einstellung der Antwortdatei unter Linux und UNIX

Eine unbeaufsichtigte Installation von CA ITCM wird von einer Antwortdatei gesteuert. Die Antwortdatei ist eine Textdatei mit Parameterwerten, die Installation und Konfiguration steuert. Die Antwortdatei wird vor der Installation manuell oder mit dem Skript "installdsm" und der Option "-g" generiert. Die Antwortdatei ist während der Installation schreibgeschützt.

Die Installation von CA ITCM umfasst standardmäßige Antwortdateien, mit denen Sie unbeaufsichtigte Installationen ausführen können. Jeder Ordner einer Komponenten enthält die Datei "install.rsp". Diese Beispielantwortdatei bietet eine vollständige Installation der Komponente.

Ändern der Werte der Installationseigenschaften

Die Antwortdatei enthält Parameterwerte (Eigenschaften), mit denen die Installation und die erste Konfiguration gesteuert werden.

Die meisten Parameter von CA ITCM haben das Präfix "CA_ITRM", "CA_DSM", "ITRM_" oder "DSM_" oder ein Präfix, das die Komponente angibt. Andere CA-Produkte können auch andere Parameter verwenden.

Sie können die Parameterwerte in der Antwortdatei unter Verwendung von "installdsm" und der Angabe "/R" außer Kraft setzen. Damit können Sie das Standardinstallationsverhalten ändern, wenn Sie mit dem Infrastructure Deployment-Assistenten oder Software Delivery-Paketen Remote-Installationen ausführen.

Gehen Sie beim manuellen Bearbeiten von Antwortdateien mit denjenigen Eigenschaftswerten sorgfältig um, die gewöhnlich von anderen Eigenschaftswerten abgeleitet werden. Hierbei handelt es sich meistens um die Speicherorte von Verzeichnissen und Unterverzeichnissen. Hartkodieren Sie keine Eigenschaftswerte, die zuvor aus einem anderen Wert abgeleitet wurden, um einen Bruch der Ableitungsbeziehung zu vermeiden.

Beispiel

SDLIBRARY (der Speicherort der Software Delivery-Bibliothek) wird standardmäßig von CA_DSM_CONFIGDATA abgeleitet (dem Speicherort der CA ITCM-Konfigurationsdaten), die wiederum von CA_ITRM_BASEDIR (dem Hauptspeicherort von CA ITCM) abgeleitet wurde. Diese Beziehungen werden in der gelieferten Antwortdatei "install.rsp" beibehalten. Wenn in einer Antwortdatei "CA_DSM_CONFIGDATA" als "CA_DSM_CONFIGDATA=/data/CA/ConfigDataLocation" und "SDLIBRARY" als "SDLIBRARY=/data/CA/SDLibrary" hartcodiert wird, werden die Ableitungsbeziehungen zwischen "CA_ITRM_BASEDIR", "CA_DSM_CONFIGDATA" und "SDLIBRARY" unterbrochen.

Hinweis: Die für das Agentenpaket spezifischen Optionen sind die Installationsparameter, die während der interaktiven Bereitstellung verwendet wurden, um auf der Seite "Agentenkonfiguration" des Infrastructure Deployment-Assistenten die zusätzlichen UNIX-Installationsoptionen anzugeben. Auf dieser Seite können Sie mehrere Installationsoptionen durch Leerzeichen getrennt eingeben, um bestehende Optionen außer Kraft zu setzen.

Grundlegende Installationseigenschaften

CA_ITRM_BASEDIR

Gibt das Installationsverzeichnis des Produkts an. In diesem Verzeichnis werden nur DSM-Komponenten gespeichert, während Komponenten, die mit anderen CA Technologies-Produkten gemeinsam verwendet werden, in einem Verzeichnis gespeichert werden, auf das die Umgebungsvariable $CASHCOMP verweist. Alle DSM-Komponenten müssen für $CA_ITRM_BASEDIR den gleichen Wert verwenden. Wenn Sie daher DSM-Agenten über den Infrastructure Deployment-Assistenten oder über die Befehlszeile eines Domänen-Managers bereitstellen, müssen Sie den erforderlichen Wert für CA_ITRM_BASEDIR in den Argumenten der DMPrimer-Komponente angeben, die normalerweise als erste DSM-Komponente auf einem Computer installiert wird. Weitere Informationen hierzu finden Sie im Abschnitt Übergabe von Optionen an die DMPrimer-Installation (siehe Seite 251).

Standard: /opt/CA/DSM

CA_DSM_CONFIGDATA

Gibt das Installationsverzeichnis für die Konfigurationsdaten an.

Standard: $CA_ITRM_BASEDIR

CASHCOMP

Gibt das übergeordnete Verzeichnis für allgemeine Komponenten und Verknüpfungsverzeichnisse an. Wenn diese Variable von anderen aktuell installierten Komponenten festgelegt wurde, wird sie nicht geändert. Die Umgebungsvariablen "$CALIB" und "$CABIN" werden von "CASHCOMP" abgeleitet. Auf einem Computer müssen alle CA Technologies-Softwarekomponenten den gleichen Wert für "$CASHCOMP" verwenden. Wenn Sie daher DSM-Agenten über den Infrastructure Deployment-Assistenten oder über die Befehlszeile eines Domänen-Managers bereitstellen, müssen Sie den erforderlichen Wert für CASHCOMP in den Argumenten der DMPrimer-Installation angeben, die normalerweise als erste DSM-Komponente auf einem Computer installiert wird. Weitere Informationen hierzu finden Sie im Abschnitt Übergabe von Optionen an die DMPrimer-Installation (siehe Seite 251).

Standard: /opt/CA/SharedComponents

DSM_ALLOW_SOFT_PREREQS

Gibt an, ob die Installation fortgesetzt werden soll, auch wenn eine Prüfung der Softwarevoraussetzungen fehlschlägt. Geben Sie "1" an, um eine Installation zu erzwingen, auch wenn die Softwarevoraussetzungen nicht erfüllt sind.

Wichtig! Wenn Sie die Voraussetzungsprüfung deaktivieren, wird CA IT Client Manager möglicherweise funktionsunfähig installiert.

Standard: 0 (Nein)

DSM_LANGUAGE

Gibt die Sprache der Installation an. Mögliche Wert sind: "enu" (Englisch/US), "deu" (Deutsch), "fra" (Französisch) und "jpn" (Japanisch). Auch wenn der Eigenschaftswert nicht "enu" ist, werden die Dateien für die ENU-Installation immer zusätzlich zu den Dateien für die angegebene Sprache installiert.

Standard: Leer (NULL). Hierdurch verwendet das Installationsprogramm das standardmäßige Gebietsschema des Systems. Wenn das Standardgebietsschema des Systems nicht unterstützt wird, wird für die Installation das Gebietsschema "enu" (Englisch/US) verwendet.

Hinweis: Die Sprache der Dialogfelder der Installationsassistenten wird von DSM_LANGUAGE nicht angegeben.

ITRM_AUTOSTART_INSTALL

Gibt an, ob nach der Installation DSM-Daemons gestartet werden. Geben Sie "0" an, wenn die DSM-Daemons nicht gestartet werden sollen.

Standard: 1 (Ja)

ITRM_AUTOSTART_REBOOT

Gibt an, ob die DSM-Daemons gestartet werden sollen, wenn der Host neu gestartet wird. Geben Sie "0" an, wenn die DSM-Daemons nicht automatisch gestartet werden sollen.

Standard: 1 (Ja)

ITRM_INST_CMDLINE

Gibt an, ob die Befehlszeilen-Hilfsprogramme zum Installieren von Software Delivery und der automatisierten Bereitstellung (DMSweep) installiert werden. Geben Sie "0" an, wenn diese Hilfsprogramme nicht installiert werden sollen.

Standard: 1 (Ja)

ITRM_SETUP_SYS_PROFILE

Gibt an, ob das Systemprofil ("/etc/profile" o. ä.) geändert werden soll, um die DSM-Umgebung für alle Anmeldebenutzer einzurichten. Geben Sie "0", wenn das System nicht geändert werden soll.

Standard: 1 (Ja)

FIPS_MODE

Gibt den FIPS-Modus von CA ITCM an. Geben Sie 1 für dem Modus "FIPS-bevorzugt" und 2 für den Modus "Nur-FIPS" ein.

Standard: 1 (FIPS-bevorzugt)

Allgemeine Agenteneigenschaften

ITRM_INST_AGENT

Gibt an, ob DSM-Agenten installiert werden sollen. Wenn dieser Parameter nicht festgelegt ist, werden Agentenfunktionen nur installiert, wenn andere Funktionen von ihnen abhängig sind. Geben Sie "0" an, wenn Agentenfunktionen nur bereitgestellt werden sollen, wenn andere Einstellungen es erfordern.

Standard: 1 (Ja)

ITRM_SERVER

Gibt den Namen des Scalability-Servers an, zu dem der DSM-Agent eine Verbindung herstellt. Dieser Parameter wird nur verwendet, wenn "$ITRM_INST_AGENT" auf "1" gesetzt ist.

Standard: *Lokaler Hostname*

ITRM_AGENT_DEFAULTGROUPS

Gibt in einer mit Kommas getrennten Liste ohne Leerzeichen an, mit welchen Managementgruppen der Agent verknüpft werden soll.

Standard: Null (impliziert, dass der Agent nicht mit Gruppen verknüpft wird)

Allgemeine Eigenschaften des Scalability-Servers (nur Linux)

ITRM_INST_SERVER

Gibt an, ob ein DSM-Scalability-Server installiert werden soll. Wenn dieser Parameter nicht festgelegt ist, werden keine Funktionen eines Scalability-Servers installiert. Dieser Parameter wird Nur-Agenten-Pakete ignoriert. Geben Sie "0" an, wenn kein Scalability-Server installiert werden soll.

Standard: 1 (Ja)

ITRM_MANAGER

Gibt den Hostnamen des Domänen-Managers an, an den der DSM-Scalability-Server seine Meldungen sendet. Dieser Parameter wird nur verwendet, wenn "$ITRM_INST_SERVER" auf "1" gesetzt ist.

Standard: *Lokaler Hostname*

Eigenschaften des Scalability-Servers (nur Linux)

ITRM_ENGINE

Gibt den Namen der Engine an, die der Scalability-Server verwendet. Ein leerer Wert gibt die System-Engine an.

Standard: Null

ITRM_PATH_COMMON_SERVER_DB

Gibt den Pfad des Datenbankverzeichnisses des Scalability-Servers an.

Standard: $CA_DSM_CONFIGDATA/Server/serverdb

Eigenschaften des Asset Management-Agenten

ITRM_INST_AM_AGENT

Gibt an, ob der Asset Management (AM)-Agent installiert werden soll. Geben Sie "0" an, wenn dieser Agent nicht installiert werden soll.

Standard: 1 (Ja)

ITRM_AMAGENT_CMDFILE_USER

Gibt die Benutzer-ID an, unter der der AM-Agent eine Befehlsdatei ausführt.

Standard: "Root"

ITRM_AMAGENT_EXTUTILITY_USER

Gibt die Benutzer-ID an, unter der der AM-Agent ein Hilfsprogramm ausführt.

Standard: "Root"

ITRM_AMAGENT_DMSCRIPT_USER

Gibt die Benutzer-ID an, unter der der AM-Agent ein DM-Skript ausführt.

Standard: "Root"

ITRM_AMAGENT_USER_INVENTORY

Gibt an, ob das Benutzerinventarmodul installiert werden soll. Geben Sie "0" an, wenn das Benutzerinventarmodul nicht installiert werden soll.

Standard: 1 (Ja)

ITRM_AMAGENT_WITHCRONINFO

Gibt an, ob crontab-Informationen angezeigt werden sollen. Geben Sie "0" an, wenn keine Informationen angezeigt werden sollen.

Standard: 1 (Ja)

ITRM_AMAGENT_WITHUSERINFO

Gibt an, ob Benutzerinformationen angezeigt werden sollen. Geben Sie "0" an, wenn keine Informationen angezeigt werden sollen.

Standard: 1 (Ja)

ITRM_AMAGENT_PRIO_LEVEL

Erhöht die Prozesspriorität von Asset Management. Der Prioritätsbereich liegt zwischen -20 und 19.

Standard: 0

ITRM_AMAGENT_EXACTINTERVAL

Gibt an, ob der AM-Agent in Intervallen (Wert = 1) oder zu festen Zeiten (Wert = 0) ausgeführt werden soll.

Standard: 1

ITRM_AMAGENT_RANDOM

Gibt an, ob der AM-Agent in bestimmten Intervallen (Wert = 0) oder in nach dem Zufallsprinzip ausgewählten Intervallen (Wert = 1) ausgeführt werden soll. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=1" festgelegt ist.

Standard: 0

ITRM_AMAGENT_WEEKLY

Gibt an, dass der AM-Agent alle n Wochen ausgeführt werden soll. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=1" festgelegt ist.

Standard: 0

ITRM_AMAGENT_DAILY

Gibt an, dass der AM-Agent alle n Tage ausgeführt werden soll. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=1" festgelegt ist.

Standard: 1

ITRM_AMAGENT_HOURLY

Gibt an, dass der AM-Agent alle n Stunden ausgeführt werden soll. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=1" festgelegt ist.

Standard: 0

ITRM_AMAGENT_EXMONDAY

Gibt an, dass der AM-Agent montags nicht ausgeführt werden soll, wenn der Wert "1" ist. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=0" festgelegt ist.

Standard: 0 (Agent wird montags ausgeführt)

ITRM_AMAGENT_EXTUESDAY

Gibt an, dass der AM-Agent dienstags nicht ausgeführt werden soll, wenn der Wert "1" ist. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=0" festgelegt ist.

Standard: 0 (Agent wird dienstags ausgeführt)

ITRM_AMAGENT_EXWEDNESDAY

Gibt an, dass der AM-Agent mittwochs nicht ausgeführt werden soll, wenn der Wert "1" ist. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=0" festgelegt ist.

Standard: 0 (Agent wird mittwochs ausgeführt)

ITRM_AMAGENT_EXTHURSDAY

Gibt an, dass der AM-Agent donnerstags nicht ausgeführt werden soll, wenn der Wert "1" ist. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=0" festgelegt ist.

Standard: 0 (Agent wird donnerstags ausgeführt)

ITRM_AMAGENT_EXFRIDAY

Gibt an, dass der AM-Agent freitags nicht ausgeführt werden soll, wenn der Wert "1" ist. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=0" festgelegt ist.

Standard: 0 (Agent wird freitags ausgeführt)

ITRM_AMAGENT_EXSATURDAY

Gibt an, dass der AM-Agent samstags nicht ausgeführt werden soll, wenn der Wert "1" ist. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=0" festgelegt ist.

Standard: 0 (Agent wird samstags ausgeführt)

ITRM_AMAGENT_EXSUNDAY

Gibt an, dass der AM-Agent sonntags nicht ausgeführt werden soll, wenn der Wert "1" ist. Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=0" festgelegt ist.

Standard: 0 (Agent wird sonntags ausgeführt)

ITRM_AMAGENT_EXECUTETIME

Gibt an, dass der AM-Agent zu dieser Uhrzeit gestartet werden soll. Die Zeitangabe hat das Format "HH:MM" (Stunde:Minute). Dieser Parameter ist nur von Bedeutung, wenn "$ITRM_AMAGENT_EXACTINTERVAL=0" festgelegt ist.

Standard: 00:00 (Mitternacht)

Allgemeine Eigenschaften von Asset Management

ITRM_INST_AM

Gibt an, ob die Asset Management (AM)-Komponente installiert werden soll. Wenn dieser Parameter nicht festgelegt ist, werden keine AM-Funktionen installiert. Geben Sie "0" an, wenn keine AM-Funktionen installiert werden sollen.

Standard: 1 (Ja)

Eigenschaften des Asset Management-Softwareverwendungs-Scalability-Servers (nur Linux)

ITRM_INST_AM_METER_SERVER

Gibt an, ob der Asset Management (AM)-Softwareverwendungs-Scalability-Server installiert werden soll. Geben Sie "0" an, wenn kein Softwareverwendungs-Scalability-Server installiert werden soll.

Standard: 1 (Ja)

Eigenschaften des Asset Management-Sektorservers (nur Linux)

ITRM_INST_AM_SECTOR_SERVER

Gibt an, ob der Asset Management (AM)-Sektorserver installiert werden soll. Geben Sie "0" an, wenn der Sektorserver nicht installiert werden soll.

Standard: 1 (Ja)

Eigenschaften von DMPrimer

ITRM_INST_DMPRIMER

Legt fest, ob der DMPrimer installiert werden soll. Geben Sie "0" an, wenn der DMPrimer nicht installiert werden soll.

Standard: 1 (Ja)

Allgemeine Eigenschaften von Data Transport Service (nur Solaris)

DTS_PPP_USER

(Wird nur auf Solaris verwendet) Gibt an, ob ein PPP-Benutzer erstellt werden soll. Dieser Parameter wird ignoriert, wenn das Protokoll "asppp" oder das Protokoll "Solstice PPP" nicht erkannt wird. Geben Sie "1" an, um einen PPP-Benutzer zu erstellen.

Standard: 0 (Nein)

Allgemeine RC-Eigenschaften (nur Linux oder Mac OS X)

ITRM_INST_RC

Gibt an, ob Remote Control-Komponenten installiert werden sollen. Wenn dieser Parameter nicht festgelegt ist, werden keine Remote Control-Funktionen installiert. Geben Sie "0" an, wenn keine Remote Control-Komponenten installiert werden sollen.

Standard: 1 (Ja)

Eigenschaften des Remote Control-Agenten (nur Linux oder Mac OS X)

ITRM_INST_RC_AGENT

Gibt an, ob der Remote Control-Agent installiert werden soll. Geben Sie "0" an, wenn der Agent nicht installiert werden soll.

Standard: 1 (Ja)

ITRM_RC_AGENT_STANDALONE

Gibt an, ob der Remote Control-Agent zentral verwaltet wird (Wert = 0) oder eigenständig ist (Wert = 1).

Standard: 0

ITRM_RC_AGENT_IN_MGMT_GROUPS

Gibt an, ob ein verwalteter Agent in Managementgruppen angezeigt wird.

Standard: 1 (Ja)

Eigenschaften des Remote Control-Scalability-Servers (nur Linux)

ITRM_INST_RC_SERVER

Gibt an, ob die Remote Control-Scalability-Serverkomponente installiert werden soll. Geben Sie "0" an, wenn kein Remote Control-Scalability-Server installiert werden soll.

Standard: 1 (Ja)

Allgemeine Eigenschaften von Software Delivery

ITRM_INST_SD

Gibt an, ob Software Delivery-Komponenten (SD) installiert werden sollen. Wenn dieser Parameter nicht festgelegt ist, werden keine SD-Funktionen installiert. Geben Sie "0" an, wenn keine SD-Komponenten installiert werden sollen.

Standard: 1 (Ja)

Eigenschaften des Software Delivery-Agenten

ITRM_INST_SD_AGENT

Gibt an, ob der Software Delivery (SD)-Agent installiert werden soll. Geben Sie "0" an, wenn der Agent nicht installiert werden soll.

Standard: 1 (Ja)

CA_DSM_REPLACE_PRE_R11_SD_AGENT

Gibt an, ob der SD-Agent der Vorgängerversion von r11 ersetzt (d. h. entfernt) werden soll oder eine Koexistenz möglich ist. Dies ist nur von Bedeutung, wenn bereits ein SD-Agent einer älteren Version als r11 auf dem System installiert ist. Geben Sie "1" an, wenn ältere Agenten entfernt werden sollen.

Standard: 0 (gleichzeitig vorhanden)

Eigenschaften des SD-Boot-Servers (nur Linux)

FIPS_MODE

Definiert den vom CA ITCM-Installationsprogramm festgelegten FIPS-Modus. Zulässige Werte sind 1 (FIPS-bevorzugt) und 2 (Nur-FIPS).

ITRM_INST_SD_BOOTSERVER

Gibt an, ob der Software Delivery (SD)-Boot-Server installiert werden soll. Normalerweise werden Scalability-Server und Boot-Server auf dem gleichen Host installiert. Geben Sie "0" an, wenn kein Boot-Server installiert werden soll.

Standard: 1 (Ja)

ITRM_BOOTSERVER_OS_INSTALL_PATH

Gibt den Speicherort der OSIM-BS-Images-Bibliothek an.

Standard: $ITRM_PATH_COMMON_SERVER_DB/SDBS/var

BOOTSERVER_ENABLED

Ermittelt, ob der Boot-Server-Dienst aktiviert werden soll. Geben Sie "0" an, um den Dienst zu deaktivieren.

Standard: 1 (Ja)

BOOTSERVER_DISABLESHARES

Gibt an, ob die SMB-Freigaben deaktiviert werden sollen. Geben Sie "0" an, um die SMB-Freigaben zu aktivieren.

Standard: 1 (Ja)

Eigenschaften des SD-Scalability-Servers (nur Linux)

ITRM_INST_SD_STAGSERVER

Gibt an, ob die Software Delivery (SD)-Scalability-Serverkomponente installiert werden soll. Normalerweise werden Scalability-Server und Boot-Server auf dem gleichen Host installiert. Geben Sie "0" an, um keinen SD-Scalability-Server zu installieren.

Standard: 1 (Ja)

SDLIBRARY

Gibt den Speicherort der Softwarepaketbibliothek an.

Standard: $CA_DSM_CONFIGDATA/sd/asm/library

ITRM_SD_EXPORT_NFS_SHARE

Gibt an, ob $SDLIBRARY als NFS-Freigabe exportiert werden soll. Geben Sie "1" an, um $SDLIBRARY zu exportieren.

Standard: 0 (Nein)

ITRM_SD_EXPORT_SAMBA_SHARE

Gibt an, ob $SDLIBRARY als Samba-Freigabe exportiert werden soll. Geben Sie "1" an, um dies als SAMBA-Freigabe zu exportieren.

Standard: 0 (Nein)

DSM_SD_INSTALL_CCS_CALENDAR

Gibt an, ob der CCS-Kalender installiert werden soll (Event Management). Nur verfügbar, wenn die CCS-Verteilung verfügbar oder bereits installiert ist. Geben Sie "1" an, um den CCS-Kalender zu installieren.

Standard: 0 (Nein)

Eigenschaften der Webkonsole (nur Linux)

ITRM_INST_WEBGUI

Legt fest, ob die Webkonsole installiert werden soll. Geben Sie "1" an, wenn die Webkonsole installiert werden soll.

Standard: 0 (Nein)

Eigenschaften der Webdienste (nur Linux)

ITRM_INST_WEBSERVICES

Gibt an, ob die Webdienste installiert werden sollen. Geben Sie "1" an, wenn die Webdienste installiert werden sollen.

Standard: 0 (Nein)

WAC_MANAGER

Gibt den Manager an, zu dem die Webdienste eine Verbindung herstellen.

Standard: *Lokaler Hostname*

DSM_TOMCAT_PORT

Gibt den TCP/IP-Port an, den der Handler auf Anforderungen überwacht.

Standard: 8090

DSM_TOMCAT_SHUT

Gibt den TCP/IP-Port an, den der Handler auf Anforderungen zum Herunterfahren überwacht.

Standard: 8095

DSM_TOMCAT_AJP

Gibt den Port an, den der Worker-Prozess auf Ajp13-Anforderungen überwacht, um Anforderungen an Out-of-Process-Workers weiterzuleiten, die das Ajpv13-Protokoll verwenden.

Standard: 8020

ITRM_AMS_WEBPORT

Gibt den Web-Port des Asset Maintenance-Systems an.

Standard: 8080

Eigenschaften des PIF-Packagers

ITRM_INST_PACKAGER

Gibt an, ob das PIF Product Software Development Kit (SDK) installiert werden soll. Das SDK kann einzeln installiert werden, unabhängig von CA ITCM. Geben Sie "0" an, wenn das SDK nicht installiert werden soll.

Standard: 1 (Ja)

Eigenschaften der Dokumentation (nur Linux)

ITRM_INST_DOC

Gibt an, ob die Dokumentation installiert werden soll. Geben Sie "0" an, wenn die Dokumentation nicht installiert werden soll.

Standard: 1 (Ja)

Installationsprotokolldateien

Jede Aktivität des Installationsprogramms in CA IT Client Manager wird in Dateien protokolliert, die das Installationsprogramm automatisch erstellt.

CA Technologies bietet ein Erfassungstool für Protokolldateien namens "dsminfo", mit dem Sie alle verfügbaren Informationen ermitteln können, die Sie zum Analysieren eines Problems mit CA ITCM benötigen.

Das Tool "dsminfo" ist auf der CA Online Support-Website verfügbar und kann unter folgender Adresse heruntergeladen werden: http://support.ca.com.

Installationsprotokolldateien unter Windows

Der Installer erstellt folgende Protokolldateitypen unter Windows:

DSMSetupxxx.log

Erstellt vom Microsoft Windows Installer (MSI) und gespeichert im Verzeichnis, das mit der Umgebungsvariable "%temp%" angegeben wird. Die Protokolldatei wird erstellt, wenn der Manager, der Scalability-Server, der DSM-Explorer und die Agenten verwendet werden. Jedes MSI-Paket erstellt eine gesonderte Protokolldatei.

TRC_*xxx*.log

Erstellt von internen Prozessen und gespeichert im Verzeichnis, das mit der Umgebungsvariable "%temp%" angegeben wird. Diese Dateien dokumentieren die Konfiguration der installierten Komponenten, z. B die Konfiguration von CAF, Manager oder Datenbank.

In den Protokolldateinamen wird die Zeichenfolge *xxx* durch den Namen der Komponente ersetzt, zu der die Protokollinformationen gehören, z. B. "DSMSetupManager.log".

Installationsprotokolldateien unter Linux und UNIX

Die Installationsprotokolldatei unter Linux und UNIX heißt anfänglich "ca-dsm.install.log". Wenn Sie die Installation ändern, heißt die Protokolldatei "ca-dsm.reinstall.log". Wenn Sie das Produkt entfernen, heißt die Protokolldatei "ca-dsm.deinstall.log".

Unter Linux und UNIX werden die Installationsprotokolldateien in folgenden Verzeichnissen gespeichert:

- /tmp
- /opt/CA/installer/log

Versionsinformationen zu installierten DSM-Komponenten

Der Installer bietet Versionsinformationen zu installierten Komponenten und Funktionen von CA IT Client Manager. Auf diese Informationen kann auch mit Hilfe des Befehls "dsmver" zugegriffen werden.

Die Versionsinformationen werden im Format M.m.b.r. angezeigt. Hierbei gilt M = Hauptversionsnummer (major release number), m = Nebenversionsnummer (minor release number), b = Build-Nummer, r = Revisions-/Patch-Nummer. Bei Version 12.0.01234.1 handelt es sich beispielsweise um Hauptversion 12, Nebenversion 0, Build 1234, Revision 1.

Um die installierten Komponenten und Funktionen anzuzeigen, geben Sie in der Befehlszeile den Befehl "dsmver" ein.

Der Befehl "dsmver" hat folgendes Format:

```
dsmver
```

Das Ausgabeformat der Versionsinformationen wird in folgendem Beispiel angezeigt:

```
Desktop and Server Management
-----------------------------------------
Explorer - Asset Management         12.0.1234.1
Explorer - Remote Control           12.0.1234.1
Explorer - Software Delivery        12.0.1234.1
Manager - Engine                    12.0.1234.1
Manager - Asset Management          12.0.1234.1
Manager - Data Transport            12.0.1234.1
Server
. . . . .
```

Kapitel 4: Post-Installationstasks

In diesem Kapitel finden Sie Informationen zum Ändern, Reparieren, Upgraden und Deinstallieren einer bestehenden Installation.

Dieses Kapitel enthält folgende Themen:

Ändern der Produktsprache nach der Installation (siehe Seite 211)
Wartung der MDB (siehe Seite 212)
Installation von SQL Bridge (siehe Seite 223)
Installation von Oracle Bridge (siehe Seite 224)
Aktivieren eines Docking-Geräts unter Windows (siehe Seite 226)
Ausführen der Agenten von der Quelle unter Windows (siehe Seite 227)
Ausführen von CA ITCM-Diensten über Benutzerkonten unter Windows (siehe Seite 228)
Importieren eigener X.509-Zertifikate in das Installations-Image (siehe Seite 229)
Ändern und Reparieren einer Installation (siehe Seite 233)
Aktualisierung einer Installation (siehe Seite 235)
Deinstallation von CA ITCM (siehe Seite 236)

Ändern der Produktsprache nach der Installation

Im Folgenden werden relevante Informationen zum Ändern der Produktsprache von CA IT Client Manager nach der Installation beschrieben:

- Es gibt verschiedene Methoden zum Ändern der Produktsprache nach der Installation:
  - Für den Explorer, den Scalability-Server und den Agenten kann die Sprache bereits installierter DSM-Komponenten nachträglich geändert werden. Führen Sie auf dem Agenten-Host den Befehl "ccnfcmda" wie folgt aus:
    `ccnfcmda -cmd SetParameterValue -ps itrm/common/localization -pn language -v` *Sprache*

    Der Wert von *Sprache* gibt die gewünschte Sprache an. Mögliche Werte sind "enu" (Englisch (USA)), "deu" (Deutsch), "fra" (Französisch) und "jpn" (Japanisch) sowie für Agenten zusätzlich "chs" (vereinfachtes Chinesisch), "esn" (Spanisch) und "kor" (Koreanisch).

    Hinweis: Für ausführlichere Information über den Ccnfcmda-Befehl zur Agentenkonfiguration tippen Sie "<command> /?" in der Befehlszeile eingeben.
  - Erstellen Sie eine abfragebasierte Richtlinie, um den Befehl "ccnfcmda", wie oben beschrieben, auszuführen.
- Die Sprache des Managers kann nach der Installation nicht mehr geändert werden.

- Beim Konfigurieren der Produktsprache von CA IT Client Manager müssen Sie sicherstellen, dass das Sprachpaket für die angegebene Sprache installiert wurde, da nicht auf Verfügbarkeit hin geprüft wird. Wurde kein Sprachpaket für die angegebene Produktsprache installiert, verwendet CA IT Client Manager wieder Englisch (USA).
- Wenn die Sprache neu konfiguriert wird, müssen Sie CA IT Client Manager mit Hilfe der Befehle "caf stop" und "caf start" stoppen bzw. neu starten, damit es den neuen Wert übernehmen kann.

Weitere Informationen:

Mehrsprachige Installation (siehe Seite 113)

Wartung der MDB

Die folgenden Aufgaben bieten Informationen zur Wartung und Synchronisierung der Management-Datenbank.

Microsoft SQL Server-MDB-Wartung

Die Datenbanktabellen von Microsoft SQL Server (SQL Server) sollten jedes Mal, nachdem die Datenbank mit größeren Datenmengen aktualisiert wurden, optimiert werden.

Zur Unterstützung bei der Verwaltung der Management-Datenbank (MDB) auf SQL Server bietet CA IT Client Manager das Wartungsskript "DsmMSSqlOpt.bat", das Administratoren regelmäßig anwenden können.

Das Skript "DsmMSSqlOpt.bat" hilft bei der Optimierung der Datenbanktabellen, indem es Wartungsaufgaben wie die Defragmentierung des Index und die Aktualisierung der Statistik ausführt. Das Skript betrifft ausschließlich CA IT Client Manager-Tabellen.

Das Wartungsskript "DsmMSSqlOpt.bat" wird während der Installation von CA IT Client Manager automatisch am folgenden Speicherort installiert:

```
%Programme$\CA\DSM\database\mdb_install\mssql\DsmMsSqlOpt.bat
```

Das Wartungsskript "DsmMSSqlOpt.bat" ist auch auf dem CA IT Client Manager-Installationsmedium (DVD) am folgenden Speicherort verfügbar:

```
Maintenance\Windows\mssql\DsmMsSqlOpt.bat
```

Das Wartungsskript "DsmMSSqlOpt.bat" kann mit den folgenden Optionen ausgeführt werden:

`DsmMsSqlOpt.bat [-pagecount=n] [-maxfrag=m] [ -usereindex] [ {local | Servername} [MDB-Name] ]`

-pagecount

Gibt die maximale Anzahl *n* der Seiten in Tabellen oder Indizes an. Tabellen oder Indizes, die mehr als die angegebene Anzahl von Seiten enthalten, werden defragmentiert. *n* ist ein numerischer Wert.

Standard: 1000

-maxfrag

Gibt den Grad *m* der Fragmentierung an. Tabellen, deren Fragmentierungsgrad der Angabe entspricht, werden defragmentiert. *m* ist ein numerischer Wert.

Standard: 10

-usereindex

Gibt an, dass Indizes neu erstellt und nicht defragmentiert werden. Das Skript "DsmMsSqlOpt" führt standardmäßig eine Defragmentierung der Indizes aus.

Wenn Sie zusätzlich zu den Domänen-Managern einen DSM-Enterprise-Manager verwenden, muss das Wartungsskript auf beiden Ebenen für die Datenbanken ausgeführt werden. CA empfiehlt, das Skript spätestens nach der Registrierung der ersten 1.000 Computer-Assets in der Domänendatenbank auszuführen. Anschließend sollte das Skript jedes Mal ausgeführt werden, nachdem weitere 5.000 Computer-Assets registriert wurden. Auf dem Enterprise-Manager muss das Skript jedes Mal ausgeführt werden, wenn 5.000 Computer-Assets von den verknüpften Domänen-Managern repliziert wurden.

Das Skript "DsmMsSqlOpt.bat" muss lokal auf dem Computer ausgeführt werden, auf dem die MDB installiert ist. Das Skript bietet zwei Optionen: Sie können Indizes neu erstellen oder defragmentieren. Vor dem Ausführen des Skripts zum Neuerstellen des Index sollten Sie alle Managerkomponenten herunterfahren, die auf die MDB zugreifen. Die DSM-Komponenten sollten neu gestartet werden, nachdem das Skript abgeschlossen wurde.

Wenn das Skript mit der Option zum Defragmentieren der Indizes aufgerufen wird, können die DSM-Komponenten weiterhin ausgeführt werden. Vorgänge, die von einem Skript initiiert werden, sind jedoch ressourcenintensiv und können die Leistung beeinträchtigen. Beachten Sie auch, dass die Defragmentierung von Indizes für umfangreiche Datenbanken mehrere Stunden dauern kann.

Planen Sie MDB-Wartungstasks daher so, dass sie ausgeführt werden, wenn die MDB wenig oder gar nicht verwendet wird. Sie können beispielsweise planen, dass das Skript einmal pro Woche nachts oder am Wochenende ausgeführt wird.

Wichtige Hinweise zur SQL Server-MDB-Wartung

Im Folgenden finden Sie Hinweise zur Wartung der Microsoft SQL Server-MDB:

- Die Variable "%TEMP%" muss auf ein geeignetes Arbeitsverzeichnis eingestellt werden, bevor Sie das Skript "DsmMsSqlOpt.bat" starten.
- Es hat sich bewährt, als erste Wartungsmaßnahme Indizes mit einem Fragmentierungsgrad von über 30 % neu zu erstellen, da Indizes weitaus schneller neu erstellt als defragmentiert werden können. Dazu müssen Sie das Skript "DsmMsSqlOpt" mit den Optionen "-usereindex" und "-maxfrag=30" ausführen, z. B.:
  ```
  DsmMsSqlOpt.bat -maxfrag=30 -usereindex
  ```
- Nach dem ersten Schritt sollten alle Tabellen, deren Fragmentierungsgrad 10 % überschreitet, defragmentiert werden. Die Defragmentierung erfolgt durch Aufruf des Skripts "DsmMsSqlOpt" mit der Option "-maxfrag=10", z. B.:
  ```
  DsmMsSqlOpt.bat -maxfrag=10
  ```

Oracle-MDB-Wartung

Um Leistungsprobleme mit der Oracle MDB zu lösen, gehen Sie wie folgt vor:

- Führen Sie in einem Oracle-SQL-Tool auf dem Solaris-Oracle-Servercomputer den folgenden Befehl aus:

  ```
  EXEC DBMS_STATS.gather_schema_stats(ownname =>'MDBADMIN', cascade =>true,
  method_opt=>'FOR ALL COLUMNS SIZE AUTO');
  ```

- Melden Sie sich bei dem Solaris-Computer mit den Oracle-Benutzeranmeldeinformationen an und führen Sie den Befehl in der Befehls-Shell aus, wie im folgenden Beispiel gezeigt:

  ```
  echo "EXEC DBMS_STATS.gather_schema_stats (ownname => 'MDBADMIN', cascade
  =>true, method_opt=>'FOR ALL COLUMNS SIZE AUTO');"|sqlplus
  sys/<pwd>@<instance> as sysdba
  ```

  In diesem Beispiel ist <*pwdt*> das Kennwort der aktuellen Oracle-Instanz, und <*Instanz*> ist der Name der aktuellen Oracle-Instanz (SID).

Weitere Informationen:

Installation einer Remote-Oracle-MDB (siehe Seite 134)

Auf die Ziel-MDB synchronisierte Objekte

Folgende Objekttypen sind auf die SQL Server- und Oracle-basierten Ziel-MDBs synchronisiert:

- **Primäre Asset- und Benutzerinformationen**
  - Erkannte Computer
  - Erkannte Benutzer
  - Erkannte Computerbenutzer (Beziehungen zwischen Computern und Benutzern)
- **Hardwareinventar**
  - Allgemeines Computerinventar
- **Softwareinventar**
  - Softwaresignaturen
  - Computer, Software-Inventar (heuristisch und auf Basis der Signaturdateien)

Erstellen des Synchronisierungstasks

Die Synchronisierung von DSM-Assets und Inventardaten mit einer SQL Server- oder Oracle-basierten Ziel-MDB wird von einem Engine-Task initiiert, der zu einer geplanten Zeit ausgeführt wird. Sie erstellen diesen Task und legen über die DSM-Explorer-GUI die Zeitplanung für den Task fest.

Der Engine-Task, der die Synchronisierung von DSM-Assets und Inventardaten mit einer vorhandenen MDB auf Microsoft SQL Server ausführt, wird auf dieselbe Weise wie alle anderen DSM-Engine-Tasks erstellt, konfiguriert, zugewiesen, geplant und ausgeführt. Wählen Sie im DSM-Explorer "Systemsteuerung", "Engines", "Alle Engines", klicken Sie mit der rechten Maustaste auf die Engine, die den Synchronisierungstask ausführen soll, und wählen Sie im Kontextmenü "Neuen Task hinzufügen". Der Assistent für neue Tasks wird geöffnet und führt Sie durch die Erstellung des Synchronisierungstasks.

Im Assistenten für neue Tasks führen Sie die folgenden Hauptschritte aus:

- Wählen Sie auf der ersten Assistentenseite in der Dropdown-Liste "Task-Typ" den Task-Typ "Datenbanksynchronisierung" aus.
- Geben Sie auf der zweiten Assistentenseite einen geeigneten Namen und eine Beschreibung für den Datenbanksynchronisierungstask ein, die den Zweck und den Typ des Tasks wiedergeben.

- Geben Sie auf der dritten Assistentenseite den Typ der Zieldatenbank und die Anmeldeinformationen für die Ziel-MDB an, wie im Abschnitt Konfigurationsoptionen für den Synchronisierungstask (siehe Seite 216) beschrieben. Sie können Ihre Einstellungen sofort überprüfen, indem Sie auf die Schaltfläche "Testverbindung" klicken. Bevor Sie diese Seite verlassen, prüft der Assistent, ob die Ziel-MDB vorhanden ist und die erforderlichen Bedingungen erfüllt sind.
- Klicken Sie auf der vierten Assistentenseite auf die Schaltfläche "Zeitplan einrichten", wenn Sie die voreingestellte Zeitplanung für den Synchronisierungstask ("Normalerweise immer ausführen") ändern möchten. Klicken Sie auf "Fertig stellen", um die voreingestellte Zeitplanung zu verwenden und den Assistenten zu beenden.

Konfigurationsoptionen des Synchronisierungstasks

Bei der Erstellung des Synchronisierungs-Tasks müssen Sie die Anmeldeinformationen (Verbindungseigenschaften) für die Ziel-MDB auf einer der Assistentenseiten "Neuen Task erstellen" angeben.

- **SQL Server-basierte Ziel-MDB:**

  Für eine SQL Server-basierte Ziel-MDB gehören zu den erforderlichen Anmeldeinformationen:

  - Servertyp der Ziel-MDB (Wert: MS SQL Server)
  - Name des Computers, der die Ziel-MDB hostet
  - Datenbankserverinstanz, Portnummer (Standard: <none>)
  - Datenbankname
  - Benutzername auf der Ziel-MDB

    Der Benutzername ist festgelegt als "ca_itrm" und kann nicht geändert werden.
  - Kennwort auf der Ziel-MDB

    Wichtig! Hier müssen Sie das Kennwort eingeben, das Sie mit Hilfe des Kennwortparameters CA_ITRM im CA ITCM-Setup festgelegt haben, als Sie ein Upgrade der SQL Server-MDB für die Synchronisierung durchgeführt haben.

- **Oracle-basierte Ziel-MDB:**

  Für eine Oracle-basierte Ziel-MDB gehören zu den erforderlichen Anmeldeinformationen:

  - Servertyp der Ziel-MDB (Wert: Oracle)
  - Name des Computers, der die Ziel-MDB hostet
  - Server-ID der Ziel-MDB (Standard: orcl)
  - Port-Nummer für die Oracle-Ziel-MDB (Standard: 1521)
  - Benutzername auf der Ziel-MDB

    Der Benutzername ist festgelegt als "ca_itrm" und kann nicht geändert werden.
  - Kennwort auf der Ziel-MDB

    Wichtig! Hier müssen Sie das Kennwort eingeben, das Sie mit Hilfe des Kennwortparameters CA_ITRM im CA ITCM-MDB-Installationsprogramm festgelegt haben, als Sie ein Upgrade der Oracle-MDB auf Solaris für die Synchronisierung durchgeführt haben.

Sie können die vorgenommenen Einstellungen sofort überprüfen, indem Sie auf dieser Assistentenseite auf die Schaltfläche "Testverbindung" klicken. Der Manager versucht dann, eine Verbindung zur Ziel-MDB aufzubauen. Das Ergebnis der Aktion wird neben der Schaltfläche "Testverbindung" angezeigt, z. B. "Verbindung erfolgreich hergestellt".

Sie können die Zeitplanung für den Synchronisierungstask konfigurieren, indem Sie auf die Schaltfläche "Zeitplan einrichten" auf der Seite "Zeitplanung" des Assistenten "Neuen Task erstellen" klicken. Die Standardeinstellung lautet "Normalerweise immer ausführen".

Optionen und Einschränkungen der Synchronisierung

Zum Ausführen des Synchronisierungstasks stehen Ihnen die folgenden Optionen zur Verfügung:

- Synchronisierung von Daten zwischen der MDB auf dem DSM-Domänen-Manager und der Ziel-MDB.
- Synchronisierung von Daten zwischen der MDB auf dem DSM-Enterprise-Manager und der Ziel-MDB. Dies beinhaltet die Synchronisierung von Daten von allen Domänen-Managern, die dem Enterprise-Manager unterstehen.

Bei der Synchronisierung bestehen die folgenden Einschränkungen:

- Sie dürfen keine Daten von einer DSM-Domänen-Manager-MDB synchronisieren, wenn der zugeordnete Enterprise-Manager bereits mit derselben Ziel-MDB synchronisiert wird. Dies würde zu einer unnötigen Datenlast im Netzwerk führen.
- Sie dürfen keine Daten von einer DSM-Enterprise-Manager-MDB synchronisieren, wenn einer der ihr zugeordneten Domänen-Manager bereits mit derselben Ziel-MDB synchronisiert wird. Dies würde zu einer unnötigen Datenlast im Netzwerk führen.

Entfernen der Synchronisierung

Wenn Sie die Synchronisierung zwischen der Microsoft SQL Server-Quell-MDB und der -Ziel-MDB entfernen möchten, müssen Sie den Synchronisierungs-Task löschen.

Beginnen Sie mit der Entfernung des Synchronisierungstasks aus dem Verzeichnis "Alle Engine-Tasks" in der Benutzeroberfläche des DSM-Explorers, während der Synchronisierungstask mit einer Engine verknüpft ist. Klicken Sie mit der rechten Maustaste auf den Engine-Task, und wählen Sie im Kontextmenü die Option "Löschen". Sie werden aufgefordert, die Entfernung des ausgewählten Elements zu bestätigen.

Der Synchronisierungs-Task wird jedoch nicht sofort entfernt. Über das Dialogfeld "Task löschen" werden Sie benachrichtigt, dass die Engine noch einmal ausgeführt werden muss, bevor der Synchronisierungs-Task entfernt wird.

Im Dialogfeld "Task löschen" können Sie auch auswählen, dass die Engine die Ziel-MDB von synchronisierten Objekten bereinigen soll. Wenn Sie diese Option nicht auswählen, bereinigt die Engine nur die Quell-MDB. Wenn Sie diese Option auswählen, wird der Status des Synchronisierungs-Tasks geändert in: "Datenbank-Cleanup durch Engine steht noch aus". Wenn der nächste geplante Cleanup-Task durch die Engine ausgeführt wurde, entfernt die Engine den Synchronisierungs-Task und die entsprechende Verknüpfung.

Deinstallation von DSM-Manager und MDB

Wenn der DSM-Manager deinstalliert wird, wird die MDB nicht deinstalliert, sondern verbleibt auf dem System.

Die MDB wird von verschiedenen CA Technologies-Produkten verwendet, die entweder lokal zusammen mit der MDB installiert sind oder die MDB remote verwenden. Wenn eines dieser CA Technologies-Produkte deinstalliert wird, heißt das nicht zwangsläufig, dass die MDB nicht mehr verwendet wird.

Wir empfehlen, dass die Deinstallation der MDB und des ausgewählten MDB-Providers nur von einem befugten Administrator ausgeführt wird, nachdem alle Implikationen der lokalen Verwendung oder Remote-Verwendung durch andere CA Technologies-Produkte berücksichtigt wurden.

Eine Microsoft SQL Server-MDB kann über den Microsoft SQL-Enterprise-Manager entfernt werden, in dem Sie die MDB-Datenbank auswählen und sie löschen. Ein weiteres Tool, das zum Löschen einer MS SQL Server-MDB verwendet werden kann, ist SQL Server Management Studio.

Verwenden Sie zum Entfernen einer Oracle-MDB das Setup-Programm, und wählen Sie "Deinstallieren", um den PIF-Produkt-Anteil des MDB-Schemas zu entfernen. Wenn Sie sich dann als "oracle" anmelden, können Sie das Oracle-dbca-Verwaltungstool verwenden, um die Datenbanktabellen zu löschen. Schließlich können alle übrigen Dateien im Ordner "../opt/CA/SharedComponents/oracle/mdb" manuell entfernt werden, indem Sie sich als "root" anmelden.

Hinweis: Weitere Informationen zur Deinstallation einer Oracle-MDB finden Sie in der *MDB-Übersicht* (die in der CA ITCM-Dokumentation (Bookshelf) enthalten ist) oder in der entsprechenden Oracle-Dokumentation.

Wenn Sie einen DSM-Manager deinstallieren, müssen Sie den Benutzer "ca_itrm" manuell aus Microsoft SQL Server entfernen. Dasselbe gilt, sofern vorhanden, für das Konto "ca_itrm_ams". Wenn der Benutzer "ca_itrm" in Microsoft SQL Server verbleibt, ist eine neue Installation von CA ITCM mit diesem SQL Server eventuell nicht möglich. Wenn CCS verwendet wurde und auch deinstalliert wird, müssen die Konten "nsmadmin" und "hostname\TNDUsers" ebenfalls aus SQL Server gelöscht werden.

Wenn Sie einen DSM-Manager deinstallieren, werden die entsprechenden Daten in der MDB nicht standardmäßig entfernt.

Der Installationsassistent von CA ITCM enthält eine Funktion, mit der Sie Daten aus der MDB entfernen können.

Wenn Sie diese Möglichkeit zum Entfernen von Daten aus der MDB aus irgendeinem Grund nicht verwenden, müssen Sie das Skript data_uninstall (siehe Seite 221) ausführen, um die MDB zu bereinigen. Dieses Skript unterstützt Microsoft SQL Server und Oracle. Die entsprechenden Versionen des Skripts, "data_uninstall.bat" (für SQL Server) und "data_uninstall.sh" (für Oracle), stehen an den folgenden Speicherorten auf der CA ITCM-Installations-DVD zur Verfügung:

- *dvdroot*\Maintenance\Windows\mssql\
- *dvdroot*\Maintenance\Windows\oracle\

Kopieren Sie alle Dateien aus dem jeweiligen Unterverzeichnis auf das lokale Managersystem, und führen Sie in der Befehlszeile das data_uninstall-Skript mit den entsprechenden Parametern aus.

Die folgende Liste enthält Szenarien und Beispiele aus der Praxis, um die Verwendung des Skripts "data_uninstall" zu veranschaulichen:

Manager endgültig entfernen

Wenn CA ITCM die einzige Anwendung war, können Sie die MDB manuell entfernen.

Andernfalls führen Sie das Skript "data_uninstall" aus und legen die Flags für -"pdata d"- und "data d" fest.

Bereinigen des Managers, um ganz von vorne anzufangen

Wenn CA ITCM die einzige Anwendung war, können Sie die MDB manuell entfernen.

Andernfalls führen Sie das Skript "data_uninstall" aus und legen die Flags für -"pdata d"- und "cdata d" fest.

Wenn Sie auch die registrierten Assets entfernen möchten, legen Sie das Argument -"asset d" fest.

Manager entfernen, aber alle Daten beibehalten

In diesem Fall müssen einige Daten entfernt werden, die sich auf Dateisystemobjekte beziehen. Führen Sie daher das Skript "data_uninstall" aus, und legen Sie das Flag -"sdonly" fest Damit werden die Verweise auf die entsprechenden Software Delivery-Dateisystemobjekte entfernt, einschließlich der OSIM- (BS-Installationsverwaltung) und Boot-Informationen.

Befehl "data_uninstall" - Löschen von Daten aus der Datenbank

Mit dem Befehl "data_uninstall" löschen Sie Daten aus der Datenbank oder prüfen die Datenbank auf registrierte Produkte und Domänen. Der Befehl "data_uninstall" unterstützt Microsoft SQL Server und Oracle.

Der Befehl hat unterschiedliche Formate:

```
data_uninstall -server Servername
    -instance Instanzname:Port-Nummer
    -database Datenbankname
    -asset {k | d }
    -pdata {k | d }
    -cdata {k | d }
    -user
    -pwd
```

Löscht Daten aus der Datenbank in Abhängigkeit von den Flags "k" oder "d" ("k" = Daten beibehalten, "d" = Daten löschen), die als Argumente angegeben werden. (Diese Verwendung wird angezeigt, wenn Sie den Befehl ohne Argumente ausführen.)

```
data_uninstall -server Servername
    -instance Instanzname:Port-Nummer
    -database Datenbankname
    -check
```

Druckt die Anzahl der in der MDB registrierten Produkte und die Anzahl der in der Datenbank registrierten Domänen.

```
data_uninstall -server Servername
    -instance Instanzname:Port-Nummer
    -database Datenbankname
    -sdonly
```

Löscht nur Software Delivery-Daten je nach dem Objekt im Dateisystem. Dieser Befehl löscht auch alle MDB-Referenzen zu OSIM- und Boot-Images.

-Server *Servername*

Gibt den Namen des lokalen RDBMS-Systems an.

Wichtig! Der Name des Datenbankservers darf zusammen mit dem Namen der Datenbankinstanz maximal 29 Zeichen lang sein.

-Instanz *Instanzname*:*Port-Nummer*

Gibt die Datenbankinstanz an, z. B. einen Microsoft SQL Server-Instanznamen. Die Angabe der Port-Nummer ist obligatorisch, ausgenommen bei einer Microsoft SQL Server-Standardinstanz. Für eine Microsoft SQL Server-Standardinstanz müssen Sie doppelte Anführungszeichen verwenden, um einen leeren Namen wie - instance "" festzulegen.

-Datenbank *Datenbankname*

Gibt bei SQL Server den Namen der Datenbank an, z. B. "mdb".

Gibt bei Oracle die SID an.

-asset {k|d}

Gibt an, ob die Registrierung von Asset-Daten aufgehoben werden soll. Mit "-asset k" werden Assets beibehalten, mit "-asset d" wird die Registrierung von Assets aufgehoben.

-pdata {k|d}

Gibt an, ob produktspezifische Daten gelöscht werden sollen. Verwenden Sie "-pdata k", um die Daten beizubehalten, und "-pdata d", um die Daten zu löschen.

-cdata {k|d}

Gibt an, ob allgemeine CA ITCM-Daten gelöscht werden sollen. Verwenden Sie "-cdata k", um die Daten beizubehalten, und "-cdata d", um allgemeine Daten zu löschen.

-Benutzer *Benutzername*

Gibt den Benutzernamen für die Verbindung zur Datenbank an, z. B. "ca_itrm".

-Pwd:*Kennwort*

Gibt das Kennwort des Benutzers an, der über "-user" angegeben wird.

-check

Prüft, ob CA Technologies-Produkte noch in der Datenbank registriert sind, und welche Domänen registriert sind.

-sdonly

Löscht nur Software Delivery-Daten, die sich auf Objekte im Dateisystem beziehen, einschließlich OSIM- und Boot-Daten.

Beispiel: Prüfen von Produkten und Domänen

Im folgenden Beispiel wird nur geprüft, ob CA Technologies-Produkte noch in der MDB-Datenbank registriert sind. Außerdem werden alle registrieren Domänen aufgeführt.

```
data_uninstall -server myMachine
    -instance ""
    -database mdb
    -check
```

Beispiel: Löschen von Daten mit Ausnahme von Assets

In diesem Beispiel werden alle CA ITCM-Daten aus der MDB-Datenbank gelöscht. Die Registrierung der Assets wird jedoch nicht aufgehoben.

```
data_uninstall -server myMachine
    -instance ""
    -database mdb
    -check
    -asset k
    -pdata d
    -cdata d
    -user ca_itrm
    -pwd myPassword
```

Die Protokolldatei "data_uninstall"

Wenn Sie das Skript "data_uninstall" ausgeführt haben, befindet sich eine Protokolldatei mit dem Namen "data_uninstall.log" je nach Betriebssystem im folgenden temporären Verzeichnis:

- Windows:
  `%TEMP%`
- Linux:
  `/tmp`

Installation von SQL Bridge

Die SQL Bridge-Synchronisierungsfunktion wird in Ihrer Anwendungsumgebung als Bestandteil der DSM-Manager-Installation installiert. Dies bedeutet, dass auf der Quellseite der SQL Bridge keine speziellen Installationsschritte erforderlich sind. Sie müssen jedoch einige Aktualisierungsschritte auf der Zielseite der SQL Bridge für die entsprechende MDB ausführen.

Upgrade der Zielseite mit der Microsoft SQL Server-MDB 1.0.4

Microsoft SQL Server MDB 1.0.4 wird mit Unicenter Asset Portfolio Management r11.3 unter Windows verwendet.

So aktualisieren Sie die Microsoft SQL Server-Ziel-MDB

1. Führen Sie das Setup *MDB installieren* von der Installations-DVD aus.

   Dieses Verfahren wendet alle MDB-Patches an, die auf der Ziel-MDB noch nicht verfügbar sind, und erstellt den Datenbankbenutzer "ca_itrm".

2. Damit Sie von der Synchronisierungsfunktion vollständig profitieren können, müssen Sie den Testfix T5D6008 für Windows herunterladen und installieren, der unter CA Support online verfügbar ist. Folgen Sie den im Testfix bereitgestellten Installationsanweisungen. T5D6008 umfasst Fixes, die für Unicenter Asset Portfolio Management r11.3 unter Windows verfügbar sind.

Upgrade der Zielseite mit der Microsoft SQL Server-MDB 1.5

Microsoft SQL Server-MDB 1.5 wird neben CA Service Desk Manager r12 unter Windows verwendet.

Führen Sie zum Aktualisieren der Ziel-Microsoft SQL Server-MDB das Setup "MDB installieren" von der CA ITCM-Installations-DVD aus.

Dieses Verfahren wendet die aktuellen MDB-Schema-Updates für DSM an, die auf der Ziel-MDB noch nicht verfügbar sind, und erstellt den Datenbankbenutzer "ca_itrm".

Installation von Oracle Bridge

Die Oracle Bridge-Synchronisierungsfunktion wird im Rahmen der DSM-Manager-Installation in Ihrer Anwendungsumgebung installiert. Dies bedeutet, dass auf der Quellseite der Oracle Bridge keine speziellen Installationsschritte erforderlich sind. Sie müssen jedoch einige Aktualisierungsschritte auf der Zielseite der Oracle Bridge für die MDB ausführen.

Upgrade der Zielseite mit der Oracle-MDB 1.5 auf Solaris

Oracle-MDB 1.5 wird neben CA Service Desk Manager r12 unter Windows verwendet.

So aktualisieren Sie die Oracle-Ziel-MDB:

1. Führen Sie das Setup "Oracle MDB Installer auf Solaris" aus, das sich auf der CA ITCM Version 12.8-Installation DVD befindet.

   Dieses Verfahren wendet die aktuellen MDB-Schema-Updates für DSM an, die auf der Ziel-MDB noch nicht verfügbar sind, und erstellt den Datenbankbenutzer "ca_itrm".

2. Fügen Sie in der "AMS.Properties"-Datei für CA Service Desk Manager den neuen Konfigurationsparameter hinzu:

   ```
   dsm_oracle_ddl=1
   ```

Beispiel

Das folgende Beispiel zeigt, wie die "AMS.Properties"-Datei aussehen sollte:

```
# Kennwort des Benutzers "ca_itrm_ams" zum Verbinden mit der DSM-
Domänendatenbank.
dsm_domain_db_password=
# Tabelleneigentümer für DSM-Tabellen, die "on the fly" erstellt werden.
# Diese Eigenschaft muss nur dann festgelegt werden, wenn die Tabellen
# nicht von "ca_itrm" erstellt wurden.
dsm_dbowner=
# Wenn r11.2 oder höher ausgeführt wird und Oracle Bridging
# unterstützt werden soll, setzen Sie den Wert von "dsm_oracle_ddl" auf 1.
dsm_oracle_ddl=1
```

Aktivieren eines Docking-Geräts unter Windows

Gelegentlich müssen die Benutzer mobiler Geräte Informationen zwischen ihrem mobilen Gerät und einem Computer austauschen oder synchronisieren. Normalerweise wird das mobile Gerät, z. B. ein Personal Digital Assistant (PDA), über eine Basisstation oder ein Docking-Gerät angeschlossen. Der Anschluss erfolgt über den seriellen Port oder den USB-Port des Computers oder direkt über eine Infrarot- oder Bluetooth-Schnittstelle.

Um den Datenaustausch zwischen dem mobilen Gerät und dem Computer über das Docking-Gerät zu ermöglichen, müssen Sie folgende Installations- und Konfigurationsschritte ausführen:

- Installieren Sie die Synchronisierungssoftware.
  - Für Windows CE-Geräte (PocketPC und Windows Mobile):

    Installieren Sie Microsoft ActiveSync (im Lieferumfang des PocketPC- oder Windows Mobile-Geräts enthalten) auf einem Zielcomputer, und schließen Sie das Gerät an diesem Computer an.

    Hinweis: Vor der Aktivierung der Unterstützung für Docking-Geräte auf einem Host-Computer muss die ActiveSync-Komponente von Microsoft installiert werden. Außerdem muss die Microsoft ActiveSync-Komponente von den Änderungen an der Umgebungsvariable PATH, die während der Installation von CA ITCM vorgenommen werden, in Kenntnis gesetzt werden. Melden Sie sich dazu nach der Installation von CA ITCM ab und wieder an.
  - Für Palm OS-Geräte:

    Installieren Sie die HotSync-Software (Palm Desktop, im Lieferumfang des Palm OS-Geräts enthalten) auf einem Zielcomputer, und schließen Sie das Palm OS-Gerät an diesen Computer an.
- Installieren Sie auf dem Zielcomputer einen Software Delivery- oder Asset Management-Agenten.
- Aktivieren Sie auf dem Manager das Proxy-Gerät für CA ITCM folgendermaßen:
  - Erstellen Sie eine neue Konfigurationsrichtlinie, z. B. "my_dockingdevice_policy", und stellen Sie den Wert des Parameters "DSM/common components/docking_devices" auf "True" (Wahr) ein.
  - Für Software Delivery stellen Sie den Wert des Parameters "DSM/Agent/Common agent/software delivery docking device" zusätzlich auf "Palm+WinCE" ein.
  - Wenden Sie die Richtlinie auf den Zielcomputer an.

- Schließen Sie bei Windows CE-Geräten das mobile Gerät erneut an den Zielcomputer an (Verbindung trennen und erneut herstellen).

  Synchronisieren Sie Palm OS-Geräte mit dem Host-PC.

- Führen Sie auf dem Zielcomputer "caf register all" aus, oder warten Sie 24 Stunden auf die automatische Registrierung.

Ausführen der Agenten von der Quelle unter Windows

Mit CA ITCM können Sie die Asset Management-, Software Delivery- und Remote Control-Agentenkomponenten für Windows über den Installationspunkt einer administrativen MSI-Netzwerkfreigabe ausführen. Diese spezifische Funktionalität wird als *Von Quelle ausführen* bezeichnet. Wenn ein Agent im Modus "Von Quelle ausführen" installiert wurde, wird die ausführbare Programmdatei vom Installationspunkt dieser administrativen Netzwerkfreigabe geladen und ausgeführt. Konfigurationsdateien, Protokolldateien usw. werden auf der lokalen Festplatte gespeichert.

Die allgemeinen CAM- und CAWIN-Komponenten müssen jetzt immer lokal installiert werden.

Nach der Installation eines Agenten im Modus "Von Quelle ausführen" muss das Agentensystem erneut gestartet werden.

So gehen Sie vor, um eine Umgebung für die Installation von Agenten im Modus "Von Quelle ausführen" einzurichten

1. Erstellen Sie ein administratives MSI-Installationsverzeichnis.

   Verwenden Sie den interaktiven Installationsassistenten, um den Ordner "WindowsProductFiles_x86" zu öffnen und "setup.exe /a" aufzurufen. Damit wird ein Installationsverzeichnis für das vollständige Produkt und seine Komponenten erstellt.

   Wenn die Agenteninstallation im Hintergrund ausgeführt werden soll oder Sie nur eine Agentenkomponente installieren möchten, wechseln Sie zu einem der Agentenverzeichnisse unter "WindowsProductFiles_x86" und führen folgenden Befehl aus:
   `msiexec /a msipackagename /qn /v*l %temp%\ITRMAdminAgt.log"`

   Hinweis: Wenn Sie den Befehl "msiexec" für mehrere Agentenpakete verwenden möchten, stellen Sie sicher, dass Sie für alle Agenten das gleiche Stammverzeichnis verwenden.

2. Erstellen Sie eine Netzwerkfreigabe für das administrative Installationsverzeichnis, das Sie gerade erstellt haben (wenn noch keine Freigabe besteht). Sie müssen sie als Null-Sitzungsfreigabe konfigurieren.

3. Installieren Sie das MSI-Paket über den Installationspunkt der administrativen Netzwerkfreigabe.

   Auf dem Zielcomputer, auf dem Sie den Agenten im Modus "Von Quelle ausführen" installieren möchten, können Sie folgenden Befehl ausführen:
   ```
   msiexec /i \\servernode\adminshare\msipackagename ADDSOURCE=ALL
   AGENT_SERVER=servername CAF_START_SERVICE=0 /qn /v*l %temp%\DSMSetupRFS.log
   ```

   Damit wird der Agent im Hintergrund gestartet.

Sie können auch eine Umgebung zum Installieren von Agenten im Modus "Von Quelle ausführen" mit der Option zur benutzerdefinierten Installation im Installationsassistenten einrichten. Starten Sie den Installationsassistenten über einen UNC-Pfad (*Serverknoten**MSI-Admin-Freigabe*\setup.exe). Folgen Sie den Dialogfeldern der benutzerdefinierten Installation, und konfigurieren Sie jeden Agenten, der von der Quelle ausgeführt werden soll.

Hinweis: Wenn sich die administrative Netzwerkfreigabe auf einem Windows 2003 Server-Host befindet, müssen Sie u. U. das Computerkonto des Agenten zur Administratorengruppe von Windows 2003 Server hinzufügen.

Ausführen von CA ITCM-Diensten über Benutzerkonten unter Windows

Obwohl das Application Framework (CAF) unter dem lokalen Systemkonto ausgeführt wird, kann es erforderlich sein, einen CA ITCM-Dienst, wie beispielsweise den Software Delivery-Agenten, unter einem Administratorkonto auszuführen. In CAF ist dies über folgende CAF-Befehlsoptionen möglich:

setcreds

Mit dem Befehl "caf setcreds" werden die Anmeldeinformationen für einen CA ITCM-Dienst festgelegt. Nur der Asset Management- und der Software Delivery-Agent werden unterstützt. Sie können diesen Befehl direkt auf der Konsole in einem Asset- oder Softwarejob verwenden, der an zahlreiche Computer gesendet wird. Sie sollten einem Job jedoch keine Klartext-Kennworte hinzufügen.

savecreds, loadcreds

Mit dem Befehl "caf savecreds" können Sie Anmeldeinformationen für unterschiedliche Computer und Dienste in einer verschlüsselten Datei speichern. Diese Datei kann an zahlreiche Computer übertragen und mit dem Befehl "caf loadcreds" angewendet werden. Mit dieser Datei können Sie unterschiedliche Administratorkennwörter für unterschiedliche Computer angeben, da jeder Eintrag in der Datei jeweils für einen Computer gilt. Der Befehl "caf loadcreds" wendet nur die Einträge für die lokalen Computer an, auf dem der Befehl ausgeführt wird.

Ausführen von CA ITCM-Diensten als Administrator

CAF verfügt über eine neue Funktion unter Windows, mit der ein CA ITCM-Dienst unter bestimmten Benutzeranmeldeinformationen ausgeführt werden kann. Dies gilt jedoch nur für Benutzer der Administratorgruppe, andere Benutzertypen werden nicht unterstützt.

So führen Sie ein Plug-in oder einen Dienst, z. B. den Dienst "sdagent", aus:

1. Öffnen Sie eine Eingabeaufforderung.
2. Legen Sie die Anmeldeinformationen für sdagent mit Hilfe des folgenden Befehls fest:
   `caf setcreds sdagent user administrator password xxx`
3. Testen Sie die Funktion, indem Sie folgenden Befehl eingeben:
   `caf start sdagent`

   Das Programm "sdagent" (sd_jexec.exe) müsste im Task-Manager als vom Administrator ausgeführt angezeigt werden.

Importieren eigener X.509-Zertifikate in das Installations-Image

CA IT Client Manager verwendet X.509-Zertifikate zur Authentifizierung zwischen seinen Client-Prozessen und Diensten, die eine Authentifizierung erfordern. Beispielsweise wird X.509 verwendet, wenn die Software Delivery-Komponente eine Verbindung zu ihrem übergeordneten Scalability-Server herstellt.

Eine CA IT Client Manager-Installation wird mit Standardzertifikaten geliefert, die mit einem CA-Root-Zertifikat signiert sind. Dieses öffentliche Root-Zertifikat wird auf jedem Knoten des Unternehmens installiert.

Wir empfehlen dringend, für jedes Enterprise ein eigenes Root-Zertifikat, Basis-Hostidentitätszertifikate (BHI) und anwendungsspezifische Zertifikate zu erstellen und bereitzustellen.

Detaillierte Informationen zum Erstellen von endanwenderspezifischen Zertifikaten finden Sie unter CA IT Client Manager-Sicherheitsfunktionen (siehe Seite 403).

Wenn Sie neue Zertifikate mit dem Tool "cacertutil" erstellen, müssen Sie mindestens eine Komponente installieren (Explorer, Asset Management-Agent usw.). Das Tool "cacertutil" befindet sich im Ordner "bin" im DSM-Installationsverzeichnis.

Wenn Sie eigene spezifische Zertifikate erstellt haben, ersetzen Sie die Standardzertifikate im Installations-Image durch Ihre eigenen neuen Zertifikate, bevor Sie DSM-Komponenten installieren oder bereitstellen.

Wenn Sie die Zertifikate im Installations-Image ersetzt haben, kann die Installation oder Bereitstellung wie üblich aufgenommen werden.

Standardzertifikate für Windows

Die Standardzertifikate für Windows befinden sich in den folgenden Ordnern. Jeder dieser Ordner verfügt über die Unterverzeichnisstruktur "Program Files\CA\DSM\bin", in der die relevanten Zertifikate enthalten sind.

- AgentBHW
- AgentAM
- AgentRC
- AgentSD
- AllAgents
- Server
- Manager
- Explorer

Standardzertifikate für Linux und UNIX

Die Standardzertifikate für Linux und UNIX befinden sich im Unterverzeichnis "certificates" der folgenden Paketverzeichnisse:

- Agent
- am_agent
- basichwinv
- rc_agent (nur Linux)
- sd_agent
- server (nur Linux)

Anpassen von X.509-Zertifikaten mit der Datei "cfcert.ini"

Die Datei "cfcert.ini" steuert die von CA ITCM installierten Zertifikate. Die Datei "cfcert.ini" enthält mehrere Abschnitte, die jeder Anwendungsgruppe in der Installation entsprechen. Im Folgenden wird die Standarddatei "cfcert.ini" dargestellt:

```
[CAF]
files=itrm_itrm_r11_root.der,basic_id.p12

[Configuration]
files=ccsm.p12

[Manager]
files=itrm_itrm_r11_cmdir_eng.p12

[Registration]
files=registration.p12

[USD.Agent]
files=itrm_itrm_r11_sd_catalog.p12

[USD.Manager]
files=itrm_dsm_r11_agent_mover.p12,itrm_dsm_r11_sd_catalog.p12



[Files]
itrm_dsm_r11_root.der=cacertutil import -i:itrm_dsm_r11_root.der -it:x509v3
basic_id.p12=cacertutil import -i:basic_id.p12 -
ip:enc:uAa8VNL4DKZlUUtFk5INPnr2RCLGb4h0 -h -t:dsmcommon
ccsm.p12=cacertutil import -i:ccsm.p12 -t:csm -
ip:enc:IWhun2x3ys7y1FM8Byk2LMs56Rr8KmXQ
itrm_dsm_r11_cmdir_eng.p12=cacertutil import -i:itrm_dsm_r11_cmdir_eng.p12 -
ip:enc:gYuzGzNcIYzWjHA6w542pW68E8FobJhv -t:dsm_cmdir_eng
itrm_dsm_r11_sd_catalog.p12=cacertutil import -i:itrm_dsm_r11_sd_catalog.p12 -
ip:enc:wdyZd4DXpx6j5otwKY0jSaOOVLLi0txQruDVOslGOlNIMZw96c85Cw -t:dsmsdcat
itrm_dsm_r11_agent_mover.p12=cacertutil import -i:itrm_dsm_r11_agent_mover.p12 -
ip:enc:sytOQtZteLopAt1CX0jIJUJcpqBWrb7G7VegY7F7udogc1c5kLIylw -t:dsmagtmv
registration.p12=cacertutil import -i:registration.p12 -
ip:enc:z5jLhmvfkaAF4DLMDp3TWuC7nG8yh3dfvmN668thfrU -t:dsm_csvr_reg
babld.p12=cacertutil import -i:babld.p12 -ip:enc:TrdWglmuNCdeOAfj2j3vMwywVbGnlIvX
-t:babld_server
dsmpwchgent.p12=cacertutil import -i:dsmpwchgent.p12 -
ip:enc:QWF8vknD5aZsU1j5RLzgt1NQgF5DcXj4v1vS4ewDzOA -t:ent_access
dsmpwchgdom.p12=cacertutil import -i:dsmpwchgdom.p12 -
ip:enc:sqb9qO2SGjbYqzIvwM7HEbx0M6UJk8Dc82EvUoDeJmE -t:dom_access
dsmpwchgrep.p12=cacertutil import -i:dsmpwchgrep.p12 -
ip:enc:x901eho57IZ19zg6g97rQetHjA1461na7nhBmJl7mcc -t:rep_access
```

```
[Tags]
dsmcommon=x509cert://DSM r11/CN=Generic Host Identity,O=Computer Associates,C=US
csm=x509cert://dsm r11/CN=Configuration and State Management,O=Computer
Associates,C=US
dsm_cmdir_eng=x509cert://dsm r11/cn=dsm directory synchronisation,o=computer
associates,c=us
dsmsdcat=x509cert://dsm r11/CN=DSM r11 Software Delivery Catalog,O=Computer
Associates,C=US
dsmagtmv=x509cert://dsm r11/CN=DSM r11 Agent Mover,O=Computer Associates,C=US
dsm_csvr_reg=x509cert://dsm r11/CN=DSM Common Server Registration,O=Computer
Associates,C=US
babld_server=x509cert://dsm r11/cn=babld server,o=computer associates,c=us
ent_access=x509cert://dsm r11/CN=Enterprise Access,O=Computer Associates,C=US
dom_access=x509cert://dsm r11/CN=Domain Access,O=Computer Associates,C=US
rep_access=x509cert://dsm r11/CN=Reporter Access,O=Computer Associates,C=US
```

Jeder Abschnitt der Datei "cfcert.ini" gibt die Zertifikate an, die vom zugeordneten Installationsprogramm installiert werden müssen. Das Installationsprogramm liest den Eintrag "files=" im zugeordneten Abschnitt der Datei "cfcert.ini" und installiert jedes aufgeführte Zertifikat über den Befehl, der im Abschnitt "[Files]" der Datei "cfcert.ini" angegeben ist.

Das Installationsprogramm des Common Application Frameworks (CAF) stellt beispielsweise fest, dass die Zertifikate "itrm_r11_dsm_root.der" und "basic_id.p12" installiert werden müssen. Im Abschnitt "[Files]" findet das CAF-Installationsprogramm in den ersten beiden Zeilen die Befehle "cacertutil", die diesen Zertifikaten zugeordnet sind, und führt diese Befehle aus.

Im Abschnitt "[Tags]" können Sie neue Zertifikate erstellen, die nicht die standardmäßigen Zertifikat-URIs verwenden. Beim Installieren eines DSM-Managerknotens lesen die Installationskomponenten diesen Abschnitt und richten Sicherheitsprofile für die benannten URIs ein. Die zuvor aufgeführten Tags und URIs sind Standardeinstellungen von CA ITCM und werden verwendet, wenn sie nicht in der Datei "cfcert.ini" vorhanden sind.

Gemäß Festlegung sind die Dateinamen, die im Eintrag "files=" jedes Abschnitts der Datei "cfcert.ini" angegeben sind, mit den Namen der zugrunde liegenden Zertifikatdatei identisch. Damit wird eine einfachere Wartung der Initialisierungsdatei "cfcert.ini" ermöglicht.

Um die Standardzertifikate gegen Ihre eigenen Zertifikate auszutauschen, ändern Sie jeden einzelnen Abschnitt und den Abschnitt "[Files]", um die neuen Zertifikatnamen und Kennwörter anzugeben.

Wichtig! Achten Sie darauf, die neuen Zertifikate mit den richtigen Tag-Namen zu importieren. Die Tags werden mit dem Schalter "-t:" angegeben. Weitere Informationen und eine Liste der verfügbaren Zertifikate finden Sie unter "Installieren anwendungsspezifischer Zertifikate (siehe Seite 412)" und "Aktuelle Zertifikate (siehe Seite 579)".

Ändern und Reparieren einer Installation

Zum Ändern oder Reparieren einer bestehenden Installation von CA ITCM führen Sie das Installationsprogramm aus. Es stehen folgende Optionen zur Verfügung:

Ändern

Hier können Sie Komponenten hinzufügen oder entfernen.

Hinweis: Achten Sie darauf, immer den Endstatus des Änderungsprozesses anzugeben. Wenn ein Manager installiert ist und Sie einen DSM-Explorer hinzufügen möchten, stellen Sie sicher, dass Sie den Manager und den DSM-Explorer geprüft haben, da dies der gewünschte Endstatus ist.

Reparieren

Hier können Sie eine bestehende Installation reparieren. Die Reparaturfunktion prüft Dateien, Registrierungsschlüssel und Verknüpfungen der ursprünglichen Installation und installiert sie erneut, wenn sie gelöscht wurden oder beschädigt sind.

Ändern einer Installation

Das Ändern einer CA ITCM-Installation bedeutet, neue Funktionen zu installieren oder installierte Funktionen zu entfernen.

So ändern Sie eine Installation:

1. Führen Sie das Setup-Programm aus, und wählen Sie die Option "CA ITCM installieren" aus.

   Der Installer ermittelt, ob eine Installation bereits vorhanden ist und zeigt das Dialogfeld "Installationsoption auswählen" an.

2. Wählen Sie "Ändern" aus.

   Das Dialogfeld "Produktfunktionen auswählen" wird angezeigt.

3. Treffen Sie Ihre Auswahl, und klicken Sie auf "Weiter".

   Das Dialogfeld "Funktionen auswählen" wird angezeigt, in dem alle verfügbaren Funktionen dargestellt sind. Die installierten Funktionen sind bereits ausgewählt.

4. Wählen Sie die zu installierenden Funktionen aus, und heben Sie die Auswahl der zu entfernenden Funktionen auf.

5. Befolgen Sie die Anleitungen des Installationsassistenten.

Wenn der Vorgang erfolgreich abgeschlossen ist, können Sie den CAF-Dienst sofort neu starten oder angeben, dass der Dienst später neu gestartet werden soll.

Ändern der Manager-Rolle

Eine Änderung der Rolle eines DSM-Managers vom Domänen-Manager zum Enterprise-Manager oder vom Enterprise-Manager zum Domänen-Manager ist mit der Funktion "Ändern" nicht möglich. Gehen Sie folgendermaßen vor, um die Rolle eines Managers zu ändern:

- Deinstallieren Sie den Manager mit der Funktion "Ändern".
- Deinstallieren Sie den Datenbankprovider und die Management-Datenbank (MDB).

  Wichtig! Lesen Sie vor der Deinstallation des Datenbankproviders die Informationen im Abschnitt "Deinstallation des Managers und der Management-Datenbank (siehe Seite 219)".

- Installieren Sie den Manager mit seiner neuen Rolle erneut über die Funktion "Ändern".

Reparieren einer Installation:

Das Reparieren einer vorhandenen CA ITCM-Installation behebt fehlende oder beschädigte Dateien, Verknüpfungen und Registrierungseinträge der vorherigen Installation.

So reparieren Sie eine Installation:

1. Führen Sie das Setup-Programm aus, und wählen Sie die Option "CA ITCM installieren" aus.

   Der Installer ermittelt, ob eine Installation bereits vorhanden ist und zeigt das Dialogfeld "Installationsoption auswählen" an.

2. Wählen Sie "Reparieren" aus.

3. Befolgen Sie die Anleitungen des Installationsassistenten.

Die Funktion "Reparieren" ersetzt keine Dateien oder Einstellungen, die während der Verwendung von CA ITCM erstellt bzw. vorgenommen wurden.

Aktualisierung einer Installation

Bei der Aktualisierung einer Installation werden Funktionen oder Komponenten aus einer höheren Version oder einer höheren Build-Nummer neu installiert, ohne dass die Alten entfernt werden. Alle aktuellen Einstellungen werden beibehalten. Die Datenbank wird nicht überschrieben.

Zur Durchführung einer Aktualisierung gibt es folgende Möglichkeiten:

Verwenden des Installationsassistenten

Führen Sie das Setup-Programm aus. Sie werden informiert, dass eine frühere Version gefunden wurde und ein Aktualisierung erfolgt.

Verwenden des DSM-Explorers und Verteilen von Paketen für eine Aktualisierung

Im DSM-Explorer können Sie die Komponenten mit Hilfe der vorregistrierten Software Delivery-Pakete verteilen. Wenn auf dem Zielcomputer eine ältere Version vorhanden ist, führt die Software Delivery-Funktionalität automatisch eine Aktualisierung durch.

Verwenden des Bereitstellungsassistenten

Im DSM-Explorer können Sie mit Hilfe des Infrastructure Deployment-Assistenten Installationspakete auf die Zielcomputer verteilen und dort installieren. Bei Zielcomputern, auf denen bereits eine frühere Version installiert ist, ist eine Aktualisierung über die Assistentenseite "Bereitstellung: Agentenkonfiguration" erforderlich. Im Eingabefeld "Zusätzliche Windows-Installationsoptionen" müssen folgende Einstellungen eingegeben werden, um eine Aktualisierung auf dem Zielcomputer anzufordern:

```
REINSTALL=ALL REINSTALLMODE=vomus
```

Direktes Aufrufen der MSI-Pakete

Wenn Sie MSI-Pakete direkt verwenden, müssen Sie folgende Parameter in die Befehlszeile aufnehmen:

```
REINSTALL=ALL, REINSTALLMODE=vomus
```

Beispiel

```
msiexec.exe /i"N:\DSM_12_0_1234_1_DVD\WindowsProductFiles_x86\AgentSD\agtsd.msi"

REINSTALL=ALL
REINSTALLMODE=vomus /l*v "%temp%\ITRMupdateSDagent.log"
```

Deinstallation von CA ITCM

Methoden zum Deinstallieren von CA ITCM oder von Teilen der CA ITCM-Installation finden Sie in den folgenden Abschnitten:

- Deinstallation von CA ITCM unter Windows (siehe Seite 237)
- Deinstallation von CA ITCM unter Linux und UNIX (siehe Seite 239)

Deinstallation von CA ITCM unter Windows

Zum Deinstallieren von CA ITCM oder Teilen von Ihm können Sie *eine* der folgenden Optionen verwenden:

- Verwenden Sie die Funktion "Software" in der Windows-Systemsteuerung.

  Mit dieser Funktion können Sie CA ITCM vollständig oder einzelne Komponenten davon entfernen. Wählen Sie in der Liste der installierten Software das entsprechende Element aus, und klicken Sie auf die Schaltfläche "Ändern/Entfernen".

- Verwenden Sie den CA ITCM-Installationsassistenten.

  setup.exe ausführen. Der Installationsassistent wird gestartet und führt Sie durch eine interaktive Deinstallation. Wählen Sie "CA ITCM installieren" aus. In einem der folgenden Dialogfelder werden die Optionen "Entfernen", "Ändern" und "Reparieren" angezeigt.

  Wenn Sie die Option "Entfernen" auswählen, wird die gesamte CA ITCM-Installation von dem System entfernt, auf dem "setup.exe" ausgeführt wurde.

  Wenn Sie die Option "Ändern" auswählen, wird eine Liste aller Komponenten und Funktionen angezeigt, die der Installer verwaltet. Die aktuell auf dem lokalen System installierten Funktionen werden geprüft. Deaktivieren Sie die Komponenten oder Funktionen (das Häkchen verschwindet), die Sie deinstallieren möchten. Die angegebenen Funktionen werden deinstalliert, wenn Sie das Dialogfeld beenden, aber die CA ITCM-Installation wird nicht entfernt.

- Führen Sie in der Befehlszeile den Befehl "msiexec /x" mit dem entsprechenden Produktcode aus.

  Die zu entfernende Komponente wird mit ihrem Produktcode (siehe Seite 238) angegeben. Mit der Option "/qn" im Befehl "msiexec" können Sie angeben, dass die Deinstallation im Hintergrund ausgeführt wird.

Unter Windows werden bei der Deinstallation über das Setup-Programm alle CA ITCM-Produkte und -Sprachpakete deinstalliert. Durch die Deinstallation einzelner MSI-Pakete über die Option "Software" in der Windows-Systemsteuerung oder Verwendung des Befehlszeilentools "msiexec" werden keine weiteren MSI-Pakete deinstalliert.

Hinweis: Nach der Deinstallation unter Windows bleiben einige Dateien, Ordner und Registrierungsschlüssel zurück. Entfernen Sie das DSM-Verzeichnis nach Abschluss der Deinstallation manuell.

Produktcodes in CA ITCM

Die installierbaren CA ITCM-Komponenten werden wie folgt anhand eines individuellen Produktcodes identifiziert:

Basisinventar-Agent (ENU und mehrsprachig):

{501C99B9–1644–4FC2–833B–E675572F8929}

Asset Management-Agent (ENU und mehrere Sprachen):

{624FA386-3A39-4EBF-9CB9-C2B484D78B29}

Data Transport Service-Agent (ENU und mehrsprachig):

{C0C44BF2–E5E0–4C02–B9D3–33C691F060EA}

Remote Control-Agent (ENU und mehrsprachig):

{84288555–A79E–4ABD–BA53–219C4D2CA20B}

Software Delivery-Agent (ENU und mehrsprachig):

{62ADA55C–1B98–431F–8618–CDF3CE4CFEEC}

Agenten-Sprachpaket DEU:

{6B511A0E-4D3C-4128-91BE-77740420FD36}

Agenten-Sprachpaket FRA:

{9DA41BF7-B1B1-46FD-9525-DEDCCACFE816}

Agenten-Sprachpaket JPN:

{A4DA5EED-B13B-4A5E-A8A1-748DE46A2607}

Agenten-Sprachpaket ESN:

{94163038-B65E-45BE-A70C-DC319C43CFF2}

Agenten-Sprachpaket KOR:

{2C300042-2857-4E6B-BC05-920CA9953D2C}

Agenten-Sprachpaket CHS:

{2D3B15F5-BBA3-4D9E-B7AB-DC2A8BD6EAD8}

Dokumentation:

{A56A74D1–E994–4447–A2C7–678C62457FA5}

Explorer:

{42C0EC64–A6E7–4FBD–A5B6–1A6AD94A2D87}

Manager:

{E981CCC3–7C44–4D04–BD38–C7A501469B37}

Master-Setup:

{C163EC47–55B6–4B06–9D03–2A720548BE86}

Scalability-Server:

{9654079C-BA1E-4628-8403-C7272FF1BD3E}

DMPrimer:

{A312C331-2E7A-42E1-9F31-902920C402EE}

Beispiel für die Deinstallation mit Hilfe von msiexec und Produktcode

Im folgenden Beispiel wird der Asset Management-Agent im Hintergrundmodus entfernt und Informationen zum Entfernen werden in die Protokolldatei "rmvamagt.log" im Protokollverzeichnis auf Laufwerk C: geschrieben.

```
msiexec /x {A302890B-3180-455B-A958-6DDFAE9F4B00} /l*v "c:\logs\rmvamagt.log" /qn
```

Deinstallation von CA ITCM unter Linux und UNIX

Sie können CA ITCM vollständig oder in Teilen unter Linux und UNIX mit einer der folgenden Optionen deinstallieren:

./setup.sh

Führen Sie "setup.sh" über die Installations-DVD aus, und wählen Sie im Setup-Dialog "Deinstallieren".

lsm -e *Produktname* [-s]

Führen Sie diese Version des Befehls "lsm" in der CA ITCM-Befehlszeile aus. Im Befehl "lsm" wird das Produkt oder die Komponente mit *prodname* angegeben. Mit der Option "-s" wird ein unbeaufsichtigter (im Hintergrund) Deinstallationsmodus angegeben.

Im folgenden Beispiel wird CA ITCM vollständig im unbeaufsichtigten Modus (Hintergrundmodus) deinstalliert:

```
lsm -e ca-dsm -s
```

Im folgenden Beispiel wird der DMPrimer deinstalliert:

```
lsm -e ca-dsm-dmprimer-standalone
```

Die Produkt- oder Komponentennamen, die als Werte für die Variable *prodname* im Linux/UNIX-Installationsbefehl (lsm) verwendet werden können, sind in der folgenden Tabelle aufgeführt:

Name des Produkts bzw. der Komponente	Beschreibung
ca-dsm	CA IT Client Manager

Name des Produkts bzw. der Komponente	Beschreibung
ca-dsm-dmprimer-standalone	DMPrimer (nur installiert bei Verwendung der Infrastructure Deployment-Komponente von CA ITCM)
ca-dsm-SMPackager	Software Packager für Linux und UNIX

Allgemeine Hinweise zur Deinstallation eines Agenten

Bei der Deinstallation des Basispakets eines Agenten werden ebenfalls alle damit verknüpften Sprachpakete entfernt.

Die Deinstallation eines Sprachpakets wirkt sich jedoch nicht auf das Agenten-Basispaket aus. Sprachpakete können also jederzeit problemlos entfernt werden.

Wenn ein eigenständiges Sprachpaket deinstalliert wird und die aktuelle Sprache im Konfigurationsspeicher (comstore) hierauf eingestellt ist, wird der Wert des Konfigurationsparameters, itrm/common/localization/language, in "comstore" in "enu" geändert. Weiter wird der Parameterwert nicht geändert.

Ein Sprachpaket hebt die Registrierung in Software Delivery und Infrastructure Deployment bei der Deinstallation selbst auf.

Software Delivery verwenden, um Windows Agent-DSM-Pakete zu deinstallieren

DSM-Pakete können in zwei Gruppen aufgeteilt werden: Basispakete und benutzerdefinierte Pakete. Benutzerdefinierte Pakete "enthalten" Basispakete, und Basispakete sind die "Atome". Basispakete werden bei Installation oder Erkennen registriert und als "installierte Software" aufgeführt. Wenn ein benutzerdefiniertes Paket mit Software Delivery geliefert und installiert wird, wird ein Installationsdatensatz für das benutzerdefinierte Paket erstellt. Dieser Installationsdatensatz für das benutzerdefinierte Paket wurde allerdings nicht für die manuelle Installation oder die Installation mittels Infrastruktur-Bereitstellung erstellt.

Wenn Sie Software Delivery verwenden, um DSM-Pakete zu deinstallieren, sollten nur Basispakete deinstalliert werden. Die Reihenfolge, in der die Basispakete deinstalliert werden sollten, ist wichtig. Deinstallieren Sie zunächst die Agenten-Sprachpakete, dann die DCS-Add-Ons, dann Asset Management und/oder Remote Control. Der Software Delivery-Agent muss selbstverständlich zuletzt deinstalliert werden. Eine Möglichkeit, dies zu implementieren, wäre das Erstellen eines Software Delivery-Deinstallations-Jobcontainers mit einem Job für jede Phase. Nachdem die Basispakete deinstalliert wurden, sollten die Installationsdatensätze der benutzerdefinierten Pakete mit DSM Explorer entfernt werden.

Beachten Sie, dass Plug-Ins wie Secure Socket Adapter und DMPrimer nicht entfernt werden. Um diese Plug-Ins zu entfernen, deinstallieren Sie manuell alle verbleibenden DSM-Komponenten auf dem Zielcomputer mit "Programme hinzufügen/entfernen".

Kapitel 5: Infrastructure Deployment

Im Folgenden werden die Infrastructure Deployment-Phasen, die Konzepte für die Bereitstellungsverwaltung und die Möglichkeiten zur interaktiven Bereitstellung über die Befehlszeile oder zur von Continuous Discovery ausgelösten Bereitstellung dargestellt. Außerdem werden einige spezielle Aspekte, Voraussetzungen und Tools der Bereitstellung berücksichtigt.

Dieses Kapitel enthält folgende Themen:

Einführung in Infrastructure Deployment (siehe Seite 244)
Bereitstellung über den DSM-Explorer (siehe Seite 258)
Bereitstellung über die Befehlszeile (siehe Seite 259)
Von Continuous Discovery ausgelöste Bereitstellung (siehe Seite 259)
Bereitstellungspakete (siehe Seite 260)
Das Tool "dsmpush" (siehe Seite 262)
Voraussetzungen für die automatische Bereitstellung der CA ITCM-Infrastruktur (siehe Seite 262)
Ändern von FTP-Serverdetails zur Verwendung mit Infrastructure Deployment (siehe Seite 266)
Windows XP-Einstellung zum Aktivieren der Bereitstellung von Agenten (siehe Seite 267)

Einführung in Infrastructure Deployment

Deployment Management (DM) ist die Infrastructure Deployment-Lösung in CA IT Client Manager. DM vereinfacht das Infrastructure Deployment von Softwarekomponenten für eine große Anzahl von Zielcomputern in einem heterogenen Enterprise. Somit wird ein Administrator zum manuellen Anmelden, Übertragen von Installations-Images, Ausführen des Installationsprozesses und Überwachen der Ergebnisse der Installation auf jedem Zielcomputer nicht mehr benötigt.

DM bietet folgende Vorteile:

- Automatisches Infrastructure Deployment für bestimmte Zielbetriebssysteme.
- Am Ende einer synchronen Bereitstellung, d. h. der Initiierung einer Bereitstellung, ist die bereitgestellte Komponente installiert und wird ohne weitere Benutzerinteraktion ausgeführt. Wenn dies nicht möglich ist, wird eine asynchrone Bereitstellung geboten, in der sich ein Benutzer möglicherweise anmelden oder das System neu starten muss, um die Installation abzuschließen.
- Erweiterte Protokollierungs- und Berichtfunktionalität. DM überwacht den Verlauf einer Bereitstellung und zeigt die entsprechenden Statusinformationen an.
- Sicherheitsfunktionen, die den Anforderungen der aktuellen Enterprise-Installationen entsprechen. Mit geeigneten Authentifizierungs- und Verschlüsselungstechnologien wird sichergestellt, dass auf sensible Daten während einer Netzwerkübertragung oder im permanenten Speicher nicht zugegriffen werden kann.
- Ein Bereitstellungs-Manager, der den größten Teil der Bereitstellungslast von den Client-Schnittstellen der Bereitstellung trennt. Bei Bedarf können mehrere Bereitstellungs-Manager auf einem einzelnen Zielcomputer bereitgestellt werden.
- Automatische Bereitstellung auf neu erkannten Systemen. Der Administrator kann Regeln zum Bereitstellen bestimmter Software auf bestimmten Systemen festlegen, wenn ein Computer zum ersten Mal im Netzwerk angezeigt wird.

Typische CA ITCM-Infrastructure Deployment-Phasen

Infrastructure Deployment umfasst die folgenden Hauptphasen:

- Interaktive Managerinstallation an den Hauptsitzen.
- Definieren der Scalability-Server für diesen Manager und Bereitstellen der Scalability-Server mit Hilfe des Bereitstellungsassistenten.
- Bereitstellen der mit den Scalability-Servern verbundenen Agenten mit Hilfe des Bereitstellungsassistenten.
- Automatische Bereitstellung auf neu erkannten Systemen.

Deployment Management-Konzepte

Wenn eine Bereitstellung angefordert wird, versucht der Manager zunächst, ein relativ kleines Primer-Paket an den Zielcomputer zu senden.

Das Primer-Paket wird mit einer von mehreren möglichen Methoden gepusht, die vom Zielbetriebssystem und der installierten Software abhängen.

Ein Remote-Push des Primers ist nicht immer möglich, beispielsweise wenn die Netzwerksicherheitseinstellungen dies verhindern. In derartigen Fällen kann der Primer jedoch manuell auf den Zielcomputern installiert werden.

Wenn der Primer installiert ist, wird er zum Übertragen der eigentlichen Bereitstellungspaketdaten auf den Zielcomputer und zum Ausführen der Installation verwendet. Alle folgenden Bereitstellungen auf demselben Zielcomputer können die bestehende Primer-Installation verwenden.

Der Bereitstellungs-Manager steuert alle Bereitstellungsvorgänge und verarbeitet des Jobstatus.

Die Bereitstellungs-Clients (Bereitstellungsassistent und Befehlszeilenschnittstelle "dmsweep") kommunizieren mit dem Bereitstellungs-Manager über eine API. Sie werden mit dem DSM-Explorer installiert und können daher bei Bedarf auch auf einem Computer ausgeführt werden, bei dem es sich nicht um den Manager handelt.

Zum Senken der Netzwerkbelastung beim Bereitstellen sehr vieler Agenten können Sie Bereitstellungspakete auf Scalability-Servern durch Staging bereitstellen.

Protokolle für die Übertragung von Paketen mit dem Scalability-Server

DMDeploy verwendet die folgenden Protokolle, um Pakete an Zielcomputer zu übertragen, wenn Sie für die Bereitstellung einen Scalability-Server verwenden:

Windows-Netzwerkfreigabe

Verwenden Sie diesen Mechanismus, wenn der Scalability-Server und der Zielcomputer unter Windows sind.

SSH/SFTP

Verwenden Sie diesen Mechanismus, wenn entweder der Scalability-Server oder der Zielcomputer unter Linux oder Unix sind.

Telnet/FTP

Verwenden Sie diesen Mechanismus, wenn entweder der Scalability-Server oder der Zielcomputer unter Linux oder Unix sind.

Weitere Informationen zu diesen Übertragungsmechanismen finden Sie unter Voraussetzungen für die automatische Bereitstellung der CA ITCM-Infrastruktur (siehe Seite 262).

Verwenden von Scalability-Servern im Kontext von Infrastructure Deployment

Zum Senken der Netzwerkbelastung beim Bereitstellen sehr vieler Agenten können Sie Bereitstellungspakete auf Scalability-Servern durch Staging bereitstellen. Um Bereitstellungsnutzdatenpakete auf einem Scalability-Server verfügbar zu machen, stellen Sie die Nutzdaten auf dem Scalability-Server bereit, aber geben die Option "Paket auf Scalability-Server durch Staging bereitstellen" an. Um anschließend Pakete bereitzustellen, die auf dem Scalability-Server gespeichert sind, aktivieren Sie die Option "Pakete vom Scalability-Server übertragen", wenn Sie die Bereitstellungsnutzdaten auswählen.

Die Verwendung eines Scalability-Servers in Verbindung mit Infrastructure Deployment wirkt sich auf die Netzwerkkonfiguration aus. Normalerweise werden über einen Scalability-Server Agenten auf Zielcomputern bereitgestellt, die sich im Enterprise-Netzwerk "in der Nähe" befinden, d. h., die Computer, die eine relativ hohe Netzwerkgeschwindigkeit zwischen dem Scalability-Server und den Agent-Computern nutzen.

Bei der Verwendung von Scalability-Servern mit Infrastructure Deployment müssen Sie einige Verwaltungstasks ausführen und beachten. Dazu gehören:

- Um sich auf Windows-Zielcomputern bereitzustellen, die einen Linux-Scalability-Server mit Telnet/FTP-Übertragungsmechanismus verwenden, müssen Sie Telnet auf Windows-Zielcomputern aktivieren. Auf Computern mit Windows 2003, Windows XP oder neueren Betriebssystemen wird der Telnet-Dienst mit Hilfe des Eintrags "Dienste" im Dialogfeld "Verwaltung" der Windows-Systemsteuerung aktiviert und gestartet.
- Zum Bereitstellen auf Linux- oder UNIX-Zielcomputern mit Hilfe eines Scalability-Servers mit Telnet/FTP-Übertragungsmechanismus muss auf dem Scalability-Server ein FTP-Server aktiviert sein. Der Zielcomputer benötigt zudem einen aktiven Telnet-Server, da der Manager über Telnet eine Verbindung zum Ziel herstellt und über FTP auf den Scalability-Server zugreift, um das Paket abzurufen.

  Wenn Ihr Scalability-Server auf einem Windows-Computer ausgeführt wird, müssen Sie außerdem auf dem Scalability-Server die folgende Konfigurationsaufgabe durchführen, um eine alternative FTP-Site für die Verwendung durch Infrastructure Deployment einzurichten. Eine separate FTP-Site ist erforderlich, um bei der gemeinsamen Verwendung des Staging-Orts, an dem CA ITCM-Agentenpakete gespeichert werden, Sicherheitsprobleme mit anderen FTP-Bereichen zu vermeiden:

- Öffnen Sie die Systemsteuerung und die Verwaltungstools, und wählen Sie "Internet-Informationsdienste".
- Klicken Sie mit der rechten Maustaste auf den Knoten "FTP-Sites", und wählen Sie "Neu", "FTP-Site", um den Assistenten für die Erstellung von FTP-Sites auszuführen.
- Führen Sie den Assistenten aus, und geben Sie als Beschreibung für die neue Site "ITCM-FTP-Site" ein. Wählen Sie die im Assistenten angegebenen Standardwerte aus, bis Sie zur Assistentenseite "Basisverzeichnis der FTP-Site" gelangen. Auf dieser Seite müssen Sie das Verzeichnis für den DMPrimer-Installationsort angeben, da dies das Verzeichnis ist, in dem ITCM Infrastructure Deployment-Agentenpakete durch Staging bereitgestellt werden. Wenn auf Ihrem Computer bereits ein DMPrimer installiert ist, suchen Sie das Verzeichnis mit Hilfe der Schaltfläche "Durchsuchen". Standardmäßig ist der DMPrimer unter "Programme\CA\DSM\DMPrimer" installiert. Fahren Sie nach der Auswahl des FTP-Site-Verzeichnisses mit dem Assistenten fort. Wählen Sie dabei die Standardoptionen aus, und klicken Sie abschließend auf die Schaltfläche "Fertig stellen".

Hinweis: Wenn Sie den Windows-Scalability-Server für die Bereitstellung auf Linux-Zielen verwenden, muss die CA ITCM-FTP-Site gestartet werden. Stellen Sie sicher, dass alle anderen FTP-Sites, z. B. die Standard-FTP-Site, beendet wurden, da anderenfalls die Bereitstellung fehlschlägt.

- Wenn Sie auf einem Scalability-Server FTP verwenden, müssen Sie beim Angeben der Benutzeranmeldeinformationen für den Verbindungsaufbau vorsichtig vorgehen. Bei der Bereitstellung eines Pakets durch Staging auf dem Scalability-Server bzw. FTP-Server müssen Sie die Anmeldeinformationen eines Benutzers angeben, der Schreibzugriff auf den Scalability-Server verfügt. Wenn Sie ein Paket über einen Scalability-Server bzw. FTP-Server bereitstellen, wird für den Zugriff auf die Pakete üblicherweise der anonyme Benutzer verwendet.
- Wenn die Bereitstellung über Telnet/FTP erforderlich ist, werden bei der Installation des Managers die Informationen zum FTP-Server angegeben, und die DMPrimer-Pakete werden auf den angegebenen Server hochgeladen. Normalerweise befindet sich der FTP-Server auf demselben Computer wie der Scalability-Server.

  Wenn mehrere FTP-Server für einen Infrastructure Deployment-Manager verwendet werden, z. B. wenn es mehrere Scalability-Server gibt, auf denen jeweils ein FTP-Server ausgeführt wird, müssen einige manuelle Konfigurationsschritte vorgenommen werden, bevor für die Bereitstellung ein alternativer FTP-Server verwendet werden kann, der zum Zeitpunkt der Installation nicht konfiguriert war.

  Um die FTP-Details zu ändern, müssen Sie den Befehl "Dmdeploy-Ftpinfo" mit den Details des neuen FTP-Servers ausführen, und die Primer-Pakete und die Datei "dmkeydat.cer" an den entsprechenden Speicherort auf dem FTP-Server kopieren. Der Bereitstellungs-Manager verwendet dann diesen FTP-Server für die Bereitstellung über Telnet/FTP. Diese Schritte werden im Abschnitt "Ändern von FTP-Serverdetails zur Verwendung mit Infrastructure Deployment (siehe Seite 266)" erläutert.

- Wenn Sie einen Scalability-Server unter Windows für die Infrastruktur-Bereitstellung verwenden, müssen Sie wissen, dass Windows über eine Begrenzung gleichzeitiger Verbindungen verfügt. Einige Jobs können fehlschlagen, wenn das Verbindungslimit erreicht wird. In diesem Fall erhalten Sie die Meldung *Das Paket kann zu diesem Zeitpunkt nicht abgerufen werden. Auf dem Scalability-Server wurde das Verbindungslimit erreicht. Wiederholen Sie den Vorgang.* Mit dem Konfigurationsparameter "Limit für Bereitstellungs-Thread" können Sie die Anzahl gleichzeitiger Bereitstellungen steuern, die vom Infrastructure Deployment-Manager ausgeführt werden. Der Standardwert des Konfigurationsparameters beträgt 10 und kann geändert werden, wenn die Bereitstellungen über einen Scalability-Server erfolgt, auf dem Windows ausgeführt wird.
- In einer reinen IPv6-Umgebung schlägt die Bereitstellung fehl, wenn die verwendeten Telnet-Versionen das IPv6-Protokoll nicht unterstützen.
- In einer reinen IPv6-Umgebung schlägt die Bereitstellung auf Linux- oder UNIX-Zielcomputern fehl, wenn die verwendeten FTP-Versionen das IPv6-Protokoll nicht unterstützen.

Weitere Informationen:

Protokolle für die Übertragung von Paketen mit dem Scalability-Server (siehe Seite 245)

Auditing von Scalability-Servern mit Infrastructure Deployment-Inhalt

In Infrastructure Deployment können Benutzer ein Auditing der Scalability-Server im Netzwerk vornehmen, die Bereitstellungsinhalte enthalten. Sie können auch eine Liste der Bereitstellungspakete abrufen, die auf jedem Scalability-Server vorhanden sind.

Die Liste der auf einem Scalability-Server verfügbaren Infrastructure Deployment-Pakete wird angezeigt, wenn der Scalability-Server während der Navigation im Bereitstellungsassistenten ausgewählt wird. Der Inhalt des Scalability-Servers kann auch über den Befehl "dmsweep sspack" angezeigt werden.

Deployment Management-Prozess

Wenn Sie Deployment Management (DM) ausführen, führen Sie die folgenden Hauptschritte des Bereitstellungsvorgangs aus:

1. Vom Administratorcomputer sendet die Infrastructure Deployment-Client-Komponente (Bereitstellungsassistent oder Befehl "dmsweep") eine Anforderung an den DM-Manager (DMDeploy), um einen Agenten auf einer Liste mit einem oder mehreren Zielcomputern zu installieren. Der Bereitstellungs-Manager kann auf einem Remote-Computer ausgeführt werden. Die Liste der Ziele kann aus expliziten Computernamen oder IPv4-Adressen bestehen oder von einem Quellcontainer, z. B. einer Windows-Domäne, einem LDAP-Verzeichnis oder einer CA ITCM-Abfrage, abgerufen werden.

   Damit die Bereitstellung auf jedem Zielcomputer erfolgreich ist, müssen Sie sicherstellen, dass der Name des Ziels (ob explizit eingegeben oder aus einem Container abgerufen) geeignet ist, die Adresse des Ziels aufzulösen, die auf dem Computer des Bereitstellungs-Managers angezeigt wird. Wenn beispielsweise die Liste der Ziele, die aus einem Verzeichnis abgerufen werden, innerhalb der Netzwerk-Domänennamen nicht vollständig qualifiziert ist, kann die Bereitstellung in bestimmten Netzwerkkonfigurationen unter Umständen nicht fortgesetzt werden.

2. Es wird geprüft, ob der DMPrimer bereits auf dem Zielcomputer installiert ist. Wenn dies nicht der Fall ist, wird DMPrimer zuerst auf dem Zielcomputer installiert. Der DM-Manager versucht, das DMPrimer-Installationspaket zu liefern. Die verwendete Übertragungsmethode hängt von der Zielbetriebsumgebung und der auf ihm aktivierten Sicherheitsstufe ab. Nachdem das DMPrimer-Image auf den Zielcomputer kopiert wurde, wird seine Installation initiiert.

   Da einige Betriebssysteme über keine Methode zum Remote-Aufruf der DMPrimer-Installation verfügen, muss möglicherweise festgelegt werden, dass das Installationsprogramm bei einem maßgeblichen Betriebssystemereignis installiert wird, beispielsweise bei einem Neustart. Dies wird als asynchrone Installation bezeichnet, da die Meldung zum Abschluss der Installation zu einem nicht angegebenen Zeitpunkt in der Zukunft asynchron empfangen wird. Die Installation des DMPrimer kann auch manuell ausgeführt werden.

3. Das DMPrimer-Installationsprogramm installiert sich selbst und die Komponente CA Message Queuing (CAM) auf dem Zielcomputer. Während der Installation hängt der FIPS-Modus des DMPrimer auf dem Zielcomputer vom FIPS-Modus des Managers ab. Der Manager gibt den FIPS-Modus als ein Installationsparameter weiter. Dieser Parameter wird auch in der Datei "dmprimer.cfg" aktualisiert, die Teil der DMPrimer-Installation ist.

   DMPrimer liest zum Start jedoch den FIPS-Modus von der Agentenkonfigurationsrichtlinie auf dem Zielcomputer. Wenn erfolgreich, aktualisiert der Primer die Datei "dmprimer.cfg" mit dem FIPS-Modus des Agenten und initialisiert in diesem Modus. Wenn keine Agenten auf dem Ziel vorhanden sind, wird DMPrimer im in der Datei "dmprimer.cfg" angegebenen Modus initialisiert.

   Hinweis: Auf den meisten Betriebssystemen muss die DMPrimer-Installation mit erhöhten Rechten ausgeführt werden.

4. Wenn der DMPrimer installiert ist und DMDeploy vom Zielcomputer das Signal erhalten hat, dass die Installation abgeschlossen ist, kann die Paketbereitstellung initiiert werden. Ein DMDeploy-Manager, der zuvor einen DMPrimer installiert oder sich bei ihm authentifiziert hat, kann Pakete bereitstellen, ohne Benutzernamen oder Kennwörter erneut bereitzustellen. Dies erfolgt über die Authentifizierung mit Hilfe von öffentlichen und privaten Schlüsseln. Sie können den Bereitstellungs-Manager zu einer erneuten Übertragung und Installation des DMPrimer zwingen, auch wenn bereits eine Version vorhanden ist. Stellen Sie hierzu die Konfigurationsrichtlinie "AlwaysDeployPrimer" über den DSM-Explorer ein.

Detaillierte Informationen zum Verwenden des Bereitstellungs-Managers über den DSM-Explorer finden Sie in der Online-Hilfe des Bereitstellungsassistenten.

Flexible Angabe von Bereitstellungszielen

Eine Datei mit Zielanmeldeinformationen wurde eingeführt, damit Sie Bereitstellungsziele flexibler angeben können. Mit Hilfe der Datei mit Zielanmeldeinformationen kann der Administrator Listen mit einzelnen Zielsystemen oder Zielsystemgruppen und ihren Anmeldeinformationen für Verbindungen erstellen und verwalten.

Dank dieser Datei mit Zielanmeldeinformationen können Benutzer ihre Bereitstellungen offline planen, bevor sie die tatsächlichen Bereitstellungsjobs initiieren. Sie können festlegen, dass die Bereitstellung in unterschiedlichen "Bereichen" eines Netzwerks erfolgen soll, indem Sie Dateien mit Anmeldeinformationen unterschiedlicher "Familien" erstellen, z. B. Dateien für die verschiedenen Abteilungen des Unternehmens.

Sie können die Datei mit Zielanmeldeinformationen mit dem Befehl "dmsweep" (und der Option "/targetcred") und dem Infrastructure Deployment-Assistenten verwenden.

Übergabe von Optionen an die DMPrimer-Installation

Sie können Optionen für die DMPrimer-Installation festlegen. So können Sie beispielsweise DMPrimer an nicht standardmäßigen Speicherorten installieren. Dies ist eine allgemeine Anforderung, da alle späteren Installationen von CA ITCM-Komponenten auf einem bestimmten Computer die Einstellungen des Speicherortes verwenden müssen, die zuerst von der DMPrimer-Installation festgelegt wurden. Wenn Sie nicht standardmäßige Installationsspeicherorte für die CA ITCM-Software verwenden, müssen Sie deshalb den Speicherort der DMPrimer-Installation mit Hilfe der unten beschriebenen Optionen festlegen, bevor die erste Bereitstellung auf einem bestimmten Zielcomputer stattfindet.

Sie können die Installationsoptionen sowohl über die Befehlszeile "dmsweep" (unter Verwendung der Option "/primerargs") als auch über den Bereitstellungsassistenten (unter Verwendung des Bereichs "Erweiterte Optionen anzeigen" der Seite "Agentenkonfiguration") eingeben.

Um DMPrimer an einem nicht standardmäßigen Speicherort zu installieren, müssen Sie folgende Argumente an die DMPrimer-Installation übergeben:

- Für die Bereitstellung auf Windows-Zielcomputern:

  `CA=x:\`*`NeuerProduktPfad`*

  `CASHCOMP=x:\`*`NeuerFreigegebenerBereich`*

Für die Bereitstellung auf Linux- oder UNIX-Zielcomputern:

`/RCA_ITRM_BASEDIR=/opt/`*`NeuerProduktPfad`*
`/RCASHCOMP=/opt/`*`NeuerFreigegebenerBereich`*

Standardmäßig verwenden DMPrimer-Installationen den gleichen FIPS-Modus wie der Manager. Sie können sich mir der Verwendung der folgenden Parameter verwendenden über den Standardwert hinwegsetzen:

Windows-Zielcomputer:

```
FIPS_MODE=1 //(FIPS-bevorzugt)
FIPS_MODE=2 //(Nur-FIPS)
```

Linux- oder UNIX-Zielcomputer:

```
/RITCM_FIPS_MODE=1 //(FIPS-bevorzugt)
/RITCM_FIPS_MODE=2 //(Nur-FIPS)
```

Hinweise zum Hinzufügen vom Windows- und UNIX-Installationsoptionen

Wenn Sie über die Seite "Agentenkonfiguration" des Infrastructure Deployment-Assistenten zusätzliche Windows-Installationsoptionen mit einem oder mehreren Leerzeichen an einen Bereitstellungsjob weitergeben, müssen die Parameterwerte ordnungsgemäß in Anführungszeichen gesetzt werden. Für jede zusätzliche Windows-Installationsoption muss der Wert in doppelte Anführungszeichen eingeschlossen werden, z. B.:

```
CA="C:\Programme\meinOrdner" CASHCOMP="C:\Programme\mydir\sharedComps"
```

In der Befehlszeile müssen bei Verwendung von "dmsweep" einzelne Parameter durch ein Komma voneinander getrennt und mit Anführungszeichen geschützt werden, wie in folgendem Beispiel gezeigt:

```
/pri "CA=\"C:\Programme\CA\test\" CASHCOMP=\"C:\Programme\CA\test\""
```

Hinweis zum Infrastructure Deployment mit Hilfe von IPv6-Adressen

Wenn Sie mit Hilfe von IPv6 eine CA IT Client Manager-Infrastruktur bereitstellen möchten, sollten Sie folgende Hinweise beachten:

- Die folgenden Bedingungen müssen erfüllt werden, bevor Infrastructure Deployment in einer IPv6-Umgebung verwendet werden kann:

  1. Der folgende Registrierungsschlüssel muss auf dem DSM-Manager auf 1 gesetzt werden:

     HKLM\System\CurrentControlSet\Services\smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)

  2. Wenden Sie zwei Hotfixupdates auf den Scalability-Server an:

     - http://support.microsoft.com/kb/947369/de-de
     - http://support.microsoft.com/kb/950092/de-de

  3. Der Hostname des Zielcomputers muss in eine globale IPv6-Adresse aufgelöst werden.

     Vergewissern Sie sich ebenfalls, dass die Inverssuche der IPv6-Adresse in den gleichen Hostnamen aufgelöst wird.

  4. Die Infrastructure Deployment-Konfigurationsrichtlinienoption "Hostnamen verwenden" muss auf "True" (Wahr) gesetzt werden.

  Hinweis: Wenn Sie Infrastructure Deployment dazu verwenden möchten, Software über einen Scalability-Server auf einem Windows 2003-Computer in einer IPv6-Umgebung bereitzustellen, müssen Sie auch die oben angegebenen Schritte 1 bis 3 auf dem vorgesehenen Windows 2003-Ziel ausführen.

  Wenn ein reines IPv6-Netzwerk diese Bedingungen nicht erfüllt, muss das DMPrimer-Paket manuell installiert werden. Weitere Informationen finden Sie im Abschnitt "Manuelle Installation der Primer-Software für Infrastructure Deployment< (siehe Seite 253)".

- Derzeit unterstützen Infrastructure Deployment und Continuous Discovery nur die Bereitstellung für IPv4-Adressbereiche.

Manuelle Installation der Primer-Software für Infrastructure Deployment

Auch wenn die automatische Bereitstellung auf den Zielcomputern nicht möglich ist, können Sie die Infrastruktursoftware bereitstellen, indem Sie die Primer-Software auf dem Zielcomputer manuell installieren. Sie können das Primer-Paket entweder physisch installieren oder die Installation über Anmeldeskripte ausführen.

Neben der Installation der Primer-Software müssen Sie einen Sicherheitsschlüssel installieren, der von dem Bereitstellungs-Manager generiert wird, mit dem Sie die Infrastruktur auf den Zielcomputern bereitstellen möchten.

Das DMPrimer-Installationsprogramm bietet Ihnen eine Option, um den FIPS-Modus für den Primer anzugeben. Wenn Sie nach der Installation den FIPS-Modus ändern möchten, aktualisieren Sie die Einstellung "FIPS_MODE" in der Datei dmprimer.cfg. DMPrimer liest zum Start jedoch den FIPS-Modus von der Agentenkonfigurationsrichtlinie auf dem Zielcomputer. Wenn erfolgreich, aktualisiert der Primer die Datei "dmprimer.cfg" mit dem FIPS-Modus des Agenten und initialisiert in diesem Modus. Wenn keine Agenten auf dem Ziel vorhanden sind, wird DMPrimer im in der Datei "dmprimer.cfg" angegebenen Modus initialisiert.

Installation von Deployment Primer unter Windows

Die Installation des Deployment Primer auf einem Windows-Zielcomputer erfordert folgende Aktionen:

- Stellen Sie den CA ITCM-Installationsdatenträger (DVD) auf dem Zielcomputer zur Verfügung, oder kopieren Sie die Primer-Setupdatei manuell auf den Zielcomputer.

  Die Primer-Setupdatei ist auf dem Installationsdatenträger so gespeichert: `"\WindowsProductFiles_x86\DMPrimer\dmsetup.exe" gespeichert.`
- Zum Installieren des Primers führen Sie "dmsetup.exe" auf dem Zielcomputer aus.

Installation von Deployment Primer unter Linux oder UNIX

Die Installation des Deployment Primer auf einem Linux- oder UNIX-Zielcomputer erfordert folgende Aktionen:

- Stellen Sie den CA ITCM-Installationsdatenträger (DVD) auf dem Zielcomputer zur Verfügung, oder kopieren Sie das Primer-Installations-Image manuell auf den Zielcomputer.

  Das Installations-Image des Primers befindet sich auf dem Installationsdatenträger im folgenden Verzeichnis:
  `/LinuxProductFiles_x86/dmprimer`
- Wechseln Sie zum Verzeichnis auf dem Zielcomputer, das das Primer-Installations-Image enthält, und führen Sie zum Installieren des Primers folgenden Installationsbefehl aus:
  `# sh installdmp`

Stellen Sie das Deployment Management-Zertifikat für eine Primer-Installation bereit

Der Bereitstellungsmanager generiert ein Zertifikat, das auf den Zielcomputer übertragen werden muss, damit der Primer auf dem Zielcomputer Bereitstellungspakete akzeptiert. Die Bereitstellungszertifikatsdatei heißt dmkeydat.cer.

Der Speicherort des Zertifikats kann bei der Installation konfiguriert werden. Sie können einen anderen Speicherort konfigurieren, wenn Sie das Zertifikat an einem sichereren Speicherort oder einem freigegebenen Speicherort ablegen möchten, der von zwei Managern, die eine Failover-Lösung bieten, verwendet wird. Im letzteren Fall können die Bereitstellungsmanager dank der gemeinsamen Verwendung des Zertifikats mit DMPrimer-Komponenten kommunizieren, die von einem der Manager geliefert wurden, ohne dass die Authentifizierungsinformationen erneut angegeben werden müssen.

Unter Windows befindet sich die Zertifikatsdatei im folgenden Verzeichnis:
`\Programme\CA\DSM\DMDeploy`

Das Zertifikat muss in den Primer-Installationsordner kopiert werden, der standardmäßig wie folgt heißt:
`\Programme\CA\DSM\DMPrimer`

Unter Linux und UNIX befindet sich das Bereitstellungszertifikat im folgenden Verzeichnis:
`/opt/CA/DSM/DMDeploy`

Das Zertifikat muss in den Primer-Installationsordner kopiert werden, der standardmäßig wie folgt heißt:
`/opt/CA/DSM/dmprimer/bin`

Bereitstellung der Agentenpakete

Um die Menge der bei der Bereitstellung von CA ITCM-Agenten über das Netzwerk übertragenen Daten zu verringern, verfügt CA ITCM über Agentenpakete, die nur Englisch unterstützen, und über Pakete mit Agenten für alle unterstützten Sprachen (mehrsprachige Agentenpakete).

Auf der Produktinstallations-DVD befinden sich die unterschiedlichen Agentenpakete in den Dateiordnern des Produkts, z. B. "WindowsProductFiles_x86".

Die Pakete mit ausschließlich englischer Sprachunterstützung sind durch das Suffix "_ENU" gekennzeichnet. Die mehrsprachigen Agentenpakete besitzen kein spezifisches Suffix.

In der Softwarepaketbibliothek sind englische Pakete (ENU) durch das Suffix "(English only Edition)" gekennzeichnet. Mehrsprachige Agentenpakete sind nicht gekennzeichnet.

Im Infrastructure Deployment-Assistenten sind englische Pakete (ENU) durch "(English only Edition) ENU" gekennzeichnet. Mehrsprachige Pakete sind mit dem Suffix "NLS (ENU,DEU,FRA,JPN)" gekennzeichnet.

Bei der Installation können Sie auswählen, ob die Pakete mit ausschließlich englischer Sprachunterstützung, die mehrsprachigen Agentenpakete oder beide in die Software Delivery-Bibliothek und den Infrastructure Deployment-Paketordner importiert werden sollen.

Wenn Sie nur eine Paketart (zum Beispiel Agentenpakete in englischer Sprache) auswählen und später auch die mehrsprachigen Agentenpakete hinzufügen möchten, müssen Sie hierzu den Befehl "dsmPush" erneut ausführen.

Für die Bereitstellung von mehrsprachigen Agenten auf Zielcomputern ist keine Standardsprache vorgesehen. Stattdessen wird die Installation in der Systemsprache des Zielcomputers ausgeführt. Um bei der Bereitstellung auf Zielcomputern explizit eine Installationssprache anzugeben, geben Sie im Infrastructure Deployment-Assistenten die Option DSM_LANGUAGE in das Feld "Geben Sie alle zusätzlichen Installationsoptionen für ... ein" ein. Die Option muss wie folgt angegeben werden ("*Sprache*" legt die Installationssprache auf dem Zielcomputer fest; gültige Werte sind "enu", "deu", "fra", "jpn", "chs", "esn" und "kor"):

DSM_LANGUAGE=*Sprache* (unter Windows)

/RDSM_LANGUAGE=*Sprache* (unter Linux und UNIX)

Wird keine Spracheinstellung angegeben, wird das Standardgebietsschema des Systems verwendet, sofern ein entsprechendes Sprachpaket verfügbar ist. Wenn es sich bei dem Standardgebietsschema des Systems um keine der unterstützten Sprachen handelt, verwendet der Installer wieder "Englisch" USA).

Auch wenn Sie Pakete über die Befehlszeile "dmsweep" für Zielcomputer bereitstellen, können Sie den Sprachparameter angeben. Geben Sie einfach mit Hilfe der Option "pparams" die Sprache an, die für CA ITCM verwendet werden soll.

Beispiel: Bereitstellen eines deutschen Windows-Agenten über die Befehlszeile

In diesem Beispiel handelt es sich bei dem deutschen Windows-Agenten um das Paket mit der Nummer 3.

```
dmsweep deploy /ip Zielcomputer /pn 3 /pparams Servername,/DSM_LANGUAGE=deu
```

Hinweis: Weitere Informationen zu zusätzlichen Installationsoptionen (auch Eigenschaften genannt), wie DSM_LANGUAGE, und deren Werte finden Sie in den Abschnitten zur Installation von CA ITCM über die Befehlszeile im Kapitel "Installation von CA ITCM".

Standardmäßig, werden alle Agentenpakete im gleichen FIPS-Modus wie der Manager installiert. Sie können sich mir der Verwendung der folgenden Parameter verwendenden über den Standardwert hinwegsetzen:

Windows-Zielcomputer:

```
FIPS_MODE=1 //(FIPS-bevorzugt)
FIPS_MODE=2 //(Nur-FIPS)
```

Linux- oder UNIX-Zielcomputer:

```
/RITCM_FIPS_MODE=1 //(FIPS-bevorzugt)
/RITCM_FIPS_MODE=2 //(Nur-FIPS)
```

Bereitstellung auf Windows Vista- und Windows 2008 Computern

Wenn die Firewall eines Zielcomputers mit dem Betriebssystem Windows Vista oder Windows 2008 deaktiviert ist und die Bereitstellung auf diesem Computer fehlschlägt, setzen Sie die folgende Registrierungsvariable, die gegebenenfalls erstellt werden muss, auf den Wert "1":

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
        System\LocalAccountTokenFilterPolicy
```

Dies ist erforderlich, weil die Benutzerkontensteuerung (UAC) in Windows Vista oder Windows 2008 lokalen Benutzern nicht automatisch Administratorrechte erteilt. Dies geschieht auch, wenn die lokalen Benutzer zur Administratorgruppe gehören.

Hinweis: Wenn Sie diesen Wert einstellen, wird die Filterung des Remote UAC Access-Tokens deaktiviert.

Das Einstellen dieses Wertes lohnt sich, wenn der Benutzer ein lokales Administratorkonto auf dem Windows Vista- oder Windows 2008-Computer hat. Für Domänenadministratoren lohnt sich diese Änderung nicht.

Wenn die Firewall eines Windows Vista- oder Windows 2008-Zielcomputers aktiviert ist, müssen zusätzlich zu den Dateifreigabe-Ports die folgenden Ports geöffnet werden, damit eine Bereitstellung auf dem Computer möglich ist:

- UDP-Ports:

4104	CAM
137, 138	Datei- und Druckerfreigabe usw.

- TCP-Ports:

135	dmdeploy
139, 445	Datei- und Druckerfreigabe usw.

Wenn die Bereitstellung noch immer fehlschlägt, müssen folgende ausgehende Regeln in der Firewall von Windows Vista oder Windows 2008 vollständig aktiviert werden:

- Remoteunterstützung
- Netzwerkermittlung
- Datei- und Druckerfreigabe
- Kernnetzwerk

Wenn der Bereitstellungsscan nach der Öffnung der oben genannten Ports und der Aktivierung der ausgehenden Regeln immer noch "Keine Antwort" zurückgibt, setzen Sie gegebenenfalls die Konfigurationsoption "Kein Anpingen von Ziel während Scan" auf "True". Diese Option befindet sich unter der Konfigurationsrichtlinie im Abschnitt "Manager\Infrastructure Deployment". Dadurch wird das Ziel beim Scannen als "Computer antwortet" markiert und die Fortsetzung der Bereitstellung ermöglicht. Obwohl dies nicht den Erfolg der Bereitstellung garantiert, ist es eine Möglichkeit, die anfänglichen Probleme bei der Verbindungsaufnahme mit dem Zielcomputer zu umgehen.

Bereitstellung über den DSM-Explorer

Der Infrastructure Deployment-Assistent unterstützt Administratoren bei der Bereitstellung von Agenten oder Scalability-Server in ihrem Unternehmen.

Der Assistent führt Sie schrittweise durch die Erstellung eines Bereitstellungsjobs. Sie können zwischen zwei Jobtypen wählen: Software auf Zielcomputern bereitstellen und Pakete auf dem Scalability-Server durch Staging bereitstellen. Wählen Sie das Paket, das bereitgestellt werden soll, in einer Liste aus und geben Sie an, ob es auf einem bestimmten Computer oder auf allen Computern in einer bestimmten Domäne, in einem IPv4-Adressbereich oder in einem Verzeichnis bereitgestellt werden soll. Der Assistent scannt anschließend die Zielcomputer, um zu ermitteln, ob die Bereitstellung auf allen Zielen möglich ist und für die Bereitstellung Anmeldeinformationen erforderlich sind.

Der Assistent zeigt auf dem Bildschirm Anleitungen für jeden Schritt und ein eigenes Hilfesystem an.

Nach Beginn des Bereitstellungsjobs können Sie den Job über die Funktion "Bereitstellungsjobstatus" in der Systemsteuerung überwachen und steuern. Weitere Informationen finden Sie in der *DSM-Explorer-Hilfe* im Abschnitt "Überwachen und Steuern von Agentenbereitstellungsjobs".

Hinweis: Bei der Installation von Agenten-Plug-in-Paketen auf Solaris-Computern in einer nicht globalen Zone, wird möglicherweise die folgende Statusmeldung im Fensterbereich "Status des Bereitstellungsjobs" angezeigt: "dmprimer konnte von SSH nicht installiert werden." Um dieses Problem zu lösen, aktualisieren Sie die IP-Adresse und den Namen des Agenten in der Hostdatei (/etc/hosts).

Bereitstellung über die Befehlszeile

Mit dem Hilfsprogramm "dmsweep" können Sie Bereitstellungsaktivitäten automatisieren und zahlreiche Tasks ausführen, die auch über den DSM-Explorer ausgeführt werden können.

Die Autorisierung zum Installieren des DMPrimer-Agenten über "dmsweep" in Windows NT-Umgebungen erfolgt in Deployment Management folgendermaßen. Das Hilfsprogramm "dmsweep" stellt mit den standardmäßigen Sicherheitsmechanismen eine Verbindung zum Bereitstellungs-Manager her. Als Benutzer von "dmsweep" muss Ihnen ein Systemadministrator die Berechtigung zum Ausführen von Bereitstellungen als Manager gewährt haben (Administratoren mit Berechtigungen auf BS-Ebene erhalten standardmäßig die Berechtigung zum Bereitstellen). Die Anmeldeinformationen für den Zielcomputer können Sie mit den Argumenten "/tu" (Benutzername) und "/tp" (Kennwort) angeben.

Von Continuous Discovery ausgelöste Bereitstellung

Die Funktion zum Bereitstellen von Software beim Erkennen neuer System basiert auf der Funktion "CA Common Services Continuous Discovery". Mit dem CA Common Services Distributed Intelligence Agent (DIA) werden jedes Mal, wenn ein neues System erkannt wird, Ereignisse abgerufen. Continuous Discovery wird aktiviert, nachdem der Benutzer mindestens eine Richtlinie erstellt hat, in der beschrieben wird, welches Paket abhängig von der IPv4-Adresse und dem Betriebssystem des Computers auf welchem Zielcomputer bereitgestellt werden soll. Die Richtlinien können im Assistenten für Continuous Discovery-Bereitstellungsrichtlinien definiert werden, der ähnlich wie der Infrastructure Deployment-Assistent aufgebaut ist.

Die Erkennungsprozess läuft folgendermaßen ab:

- Ein System stellt zum ersten Mal eine Verbindung zum Netzwerk her.
- Der Continuous Discovery-Dienst erkennt die neue Hardware, klassifiziert sie mit Hilfe seiner Heuristik und erstellt ein verwaltetes Objekt, welches das System im WorldView-Repository darstellt.
- Als Reaktion auf die neuen Daten in der Datenbank wird ein Trigger ausgeführt, der das Ereignis in einer speziellen (dedizierten) Ereignistabelle registriert.
- Die CA ITCM-Discovery-Anwendung, die diese Ereignisse abonniert hat, wird benachrichtigt.
- Die Discovery-Anwendung prüft mit Hilfe der Continuous Discovery-Richtlinien, ob das erkannte System ein geeignetes Ziel für neue Software ist, und ruft die Bereitstellungsschnittstelle ähnlich wie DMSweep auf.

Hinweis: Konfigurieren Sie für die Continuous Discovery-Funktion Microsoft SQL Server mit Port 1433 als Standard-Port im Domänenmanager.

Bereitstellungspakete

Folgende Bereitstellungspakete werden zur Verfügung gestellt:

- CA DSM-Agent + Basisinventar-Plug-in
- CA DSM-Agent + Asset Management-Plug-in
- CA DSM-Agent + Remote Control-Plug-in
- CA DSM-Agent + Software Delivery-Plug-in
- CA DSM Agent + AM, RC, SD Plug-in(s)

  Hierbei handelt es sich um ein Kombinationspaket, das die Agenten-Plug-ins für Basisinventar, Asset Management, Remote Control und Software Delivery beinhaltet.

  Das Linux-Paket enthält zusätzlich das CA Data Transport-Agenten-Plug-in.
- CA DSM-Scalability-Server

  Dieses Paket ist ein kombiniertes Paket, das den Scalability-Server und die Agenten-Plug-ins für Basisinventar, Asset Management, Remote Control und CA Data Transport enthält.

  Hinweis: Wenn das CA DSM Scalability-Server-Bereitstellungspaket per DMDeploy bereitgestellt wird, werden das Scalability-Server-Plug-in und *alle* Agenten-Plug-ins installiert. Wenn dieses Paket jedoch mit der Software Delivery-Funktionalität bereitgestellt wird, werden nur die Scalability-Server-, Software Delivery- und CA Data Transport-Agenten-Plug-ins installiert.

  Hinweis: Weitere Informationen über "CA DSM Scalability Server Linux (Intel)-Bereitstellungspaket, finden Sie unter Installation von "Scalability Server" unter Linux (siehe Seite 148).
- Für die Bereitstellung des Device Compliance Scanner (DCS) stehen die folgenden Bereitstellungspakete zur Verfügung:

  Windows

  - CA DSM Agent AM DCS-Plug-in (nur englische Version)
  - CA DSM Agent AM DCS-Plug-in
- Für die Bereitstellung von Remote-Virtualisierungsinventar stehen die folgenden Bereitstellungspakete zur Verfügung:

  Windows

  - CA DSM Agent AM RVI-Plug-in (nur englische Version)
  - DSM-Agent CA BIN RVI-Plug-in

  AIX

  - CA DSM Agent AM RVI-Plug-in AIX(RS/6000) (ENU)

  HP-UX

- CA DSM Agent AM RVI-Plug-in HP-UX(800) (ENU)

Linux

- CA DSM Agent AM RVI-Plug-in Linux(intel) (ENU)

Solaris Sparc

- CA DSM Agent AM RVI-Plug-in Solaris-Sparc (ENU)

Hinweis: Mit den bereitgestellten Client-Paketen wird keine CA ITCM-Dokumentation installiert.

Die Bereitstellungspakete sind nur dann auf einem Manager-Computer vorhanden, wenn die Manager-Funktion für Deployment auf dem lokalen System installiert ist (Standardinstallation).

Sie können den voreingestellten Speicherort für die Bereitstellungspakete während der Interviewphase der Installation ändern.

Wichtig! Zwar können Sie zusätzliche MSI-Befehlszeileneigenschaften für Windows-Bereitstellungspakete angeben, berücksichtigen Sie jedoch besonders die Windows-Versionen der Pakete "CA DSM Agent + AM, RC, SD Plug-in(s)" sowie "CA DSM Scalability Server". Für diese kombinierten MSI-Pakete dürfen keine paketspezifischen Eigenschaften der MSI-Funktionsliste wie "ADDLOCAL" angegeben werden, sonst schlägt die Bereitstellung des Pakets fehl. Wenn Sie paketspezifische Funktionen auflisten müssen, sollten Sie dies jeweils für das betreffende Agenten-Bereitstellungspaket tun.

Das Tool "dsmpush"

Mit dem Tool "dsmPush" können Sie Installationspakete von der Installations-DVD auf den Domänen-Manager importieren bzw. "pushen". Mit dem Tool "dsmPush" werden Pakete importiert, die zur Verwendung durch die Funktionalität "Infrastructure Deployment" oder die Funktionalität "Software Delivery" geeignet sind.

Normalerweise wurden die Pakete bereits während des Setups auf einen Manager-Computer gepusht, aber dieser Push ist optional. Wenn Sie die Pakete wieder pushen müssen, um mehr Pakete hinzuzufügen oder die Pakete zu aktualisieren, können Sie dazu das Tool "dsmpush" verwenden.

Das Werkzeug "dsmpush" bietet eine Prüffunktion und eine Kopierfunktion. Die Prüffunktion validiert vorhandene Bereitstellungspakete im Manager und listet sie auf. Über die Funktion "copy" werden mehrere Pakete für die angegebenen Produkte und Betriebssystemumgebungen in die Infrastructure Deployment-Bibliothek auf dem lokalen System oder in die Software Delivery-Bibliothek importiert.

Bei jeder Ausführung speichert das Tool "dsmpush" Protokollinformationen in die Protokolldatei " TRC_Inst_dsmPush.*ttmmjjjhhmmss*.log". " *ttmmjjjhhmmss*" ist der Zeitstempel der jeweiligen Protokolldatei.

Beachten Sie die Beschreibung der Überprüfungs- und Copy-Funktionen von "dsmpush" und ihrer Parameter im *CLI-Referenzhandbuch*.

Voraussetzungen für die automatische Bereitstellung der CA ITCM-Infrastruktur

Mit der Komponente "Infrastructure Deployment" können Sie eine Remote-Installation der Agenten- und Serversoftware auf Zielcomputern ausführen, auf denen die CA ITCM-Software nicht ausgeführt wird. Dies ist nur möglich, wenn Sie die Funktionen der zugrunde liegenden Betriebssysteme auf den Ausgangs- und Zielcomputern verwenden. Dabei gelten die Einschränkungen der Enterprise-Netzwerkkonfiguration.

Der erste Schritt beim Bereitstellen der Infrastruktursoftware ist die Remote-Installation der kleinen Primer-Anwendung DMPrimer auf dem Zielcomputer. Die DMPrimer-Software ist für die anschließende Übertragung der Installations-Images der Infrastruktursoftwarekomponente und das Aufrufen ihrer Installation zuständig. Wenn DMPrimer an die Zielcomputer geliefert wird, muss der Bereitstellungs-Manager Benutzeranmeldeinformationen angeben, die auf dem Ziel gültig sind.

Der DMPrimer wird mit einem der folgenden Mechanismen auf das Zielsystem übertragen. Wenn dem Bereitstellungs-Manager das Betriebssystem des Zielcomputers bekannt ist, wird ein entsprechender Übertragungsmechanismus ausgewählt. Wenn das Zielbetriebssystem nicht festgestellt werden kann, wird jeder der folgenden Mechanismen versucht.

- **Öffnen einer Netzwerkfreigabe**

  Der Bereitstellungs-Manager versucht, eine Verbindung zu einer Windows-Netzwerkfreigabe auf dem Zielsystem herzustellen. Der Standardname der Freigabe lautet ADMIN$, er kann jedoch über die Konfigurationsrichtlinie "defaultTargetShare" geändert werden. Dieser Mechanismus ist nur in Bereitstellungs-Managern verfügbar, die auf einer Windows-Plattform ausgeführt werden und funktioniert nur auf einigen Windows-Zielsystemen. Einige Varianten von Windows, z. B. Windows XP Home, unterstützten diesen Bereitstellungsmechanismus nicht.

- **Öffnen einer Netzwerkverbindung zum Zielcomputer mit Hilfe des SSH-Protokolls und Übertragen des Primer-Installationspakets mit Hilfe von SFTP**

  Dieser Mechanismus funktioniert auf jedem Computer, auf dem ein SSH-Server ausgeführt wird. Er wird jedoch überwiegend verwendet, wenn Linux- oder UNIX-Computer das Ziel sind.

  Hinweis: Für die Bereitstellung in Solaris-Systemen empfiehlt CA die Verwendung von SunSSH v1.1 (oder höher) oder die aktuelle Version von OpenSSH. Zusätzliche Informationen zu Patches für Solaris-Plattformen und Versionen finden Sie auf der Website unter http://opensolaris.org/os/community/security/projects/SSH.

  Wenn Sie auf dem Zielcomputer eine Firewall ausführen, stellen Sie sicher, dass der SSH-Port (22) Verbindungen vom Bereitstellungs-Manager zulässt. Sie sollten auch überprüfen, ob der SSH-Server auf dem Zielcomputer für die Verwendung eines RSA-Schlüssels mit 3DES-Verschlüsselungscode und HMAC-SHA1-Nachrichtenauthentifizierungscode (MAC) konfiguriert ist. Zwar bieten die meisten SSH-Server keine standardmäßige Unterstützung dieser Konfiguration, Anweisungen zum Hinzufügen der Unterstützung finden Sie jedoch in der Dokumentation Ihres SSH-Servers.

  Um erfolgreich auf einem UNIX- oder Linux-Agenten bereitzustellen, konfigurieren Sie die Konfigurationsdatei /etc/ssh/sshd_config Ihrer letzten SSH-Implementierung folgendermaßen:

  - Legen Sie "PasswordAuthentication" auf "Ja" fest.
  - Legen Sie "PermitRootLogin" auf "Ja" fest.
  - Prüfen Sie, ob das SFTP-Subsystem aktiviert wird

  Bei der Bereitstellung auf manchen IBM AIX-Systemen, die ein IPv4- und ein IPv6-Stack ausführen und eine IPv6-Adresse verwenden, überwacht der SSH-Server des Zielcomputers möglicherweise nur dem Port 22 auf IPv4. Hierdurch würde die Bereitstellung fehlschlagen. Bearbeiten Sie die Konfigurationsdatei "sshd_config", und setzen Sie ListenAddress auf "::", um dies zu korrigieren.

  Wenn Solaris 11 bereitgestellt wird, führen Sie diese Schritten aus:

  - Kommentieren Sie Folgendes aus:

    ```
    CONSOLE=/dev/console
    ```

  - Fügen Sie Folgendes in die Zeile ein:

    ```
    /etc/default/login.

    vi /etc/default/login

    #CONSOLE=/dev/console
    ```

  - Entfernen Sie Folgendes aus der Stammeingabe in "/etc/user_attr":

    ```
    ;type=role
    ```

    oder verwenden Sie folgenden Befehl:

    ```
    rolemod -K type=normal root
    ```

- Starten Sie den ssh-Dienst neu

  Hinweis: Wenn Sie möchten, dass die SSH-Kommunikation zwischen dem Bereitstellungsmanager und den Zielcomputer FIPS-kompatibel ist, müssen Sie überprüfen, ob der auf dem Zielcomputer ausgeführte SSH-Server ein FIPS-kompatibles kryptographisches Modul verwendet, und dass der Modus des Bereitstellungsmanagers als "Nur-FIPS" festgelegt ist.

- **Öffnen einer Netzwerkverbindung zum Zielcomputer mit Hilfe des Telnet-Protokolls und Übertragen des Primer-Installationspakets mit Hilfe von FTP**

  Dieser Mechanismus ist besonders geeignet, wenn UNIX-Systeme, die SSH nicht unterstützen, das Ziel sind. Telnet und FTP werden immer seltener verwendet, da diese Protokolle inhärente Sicherheitsschwachstellen aufweisen. Sie werden durch SSH und SFTP ersetzt.

  Wenn Sie diese Verbindungsmethode verwenden, werden auf Zielcomputern Telnet-Befehle ausgeführt, die das DMPrimer-Installations-Image von einem FTP-Server im Manager abrufen.

Wichtig! Einige neue Betriebssysteme lassen die Remote-Installation von Software nicht zu oder verhindern sie sogar. Wenn Sie versuchen, CA ITCM-Software auf diesen Systemen bereitzustellen, schlägt die Bereitstellung normalerweise mit dem Status "Kein Primer-Transport" fehl. In solchen Fällen kann die Installation von CA ITCM-Softwarekomponenten auf anderem Wege erfolgen, beispielsweise mit Installationsdatenträgern wie DVDs.

Sie können die Installation von DMPrimer auch manuell ausführen. Damit wird die Bereitstellung der CA ITCM-Infrastruktur möglich, ohne dass Sie die Funktionen der zugrunde liegenden Betriebssysteme nutzen müssen.

Ermitteln Sie, ob in Ihrer Umgebung eine automatische Bereitstellung möglich ist, indem Sie einige einfache Tests über folgende standardmäßige Betriebsystemvorgänge ausführen:

- Für die Lieferung des DMPrimer-Images mit Hilfe von Windows-Freigaben müssen Sie in der Lage sein, eine Freigabe (Standard: Admin$) vom Host-Computer Ihres Bereitstellungs-Managers jedem Bereitstellungszielcomputer zuzuordnen. Diese Zuordnung erfolgt unter Verwendung der in der Bereitstellungsanforderung angegebenen Zielbenutzer-Anmeldeinformationen.
- Für die Lieferung des DMPrimer-Images mit Hilfe von SSH müssen Sie in der Lage sein, mit SSH eine Verbindung zwischen dem Bereitstellungs-Manager und den Bereitstellungszielcomputern herzustellen.
- Für die Lieferung von DMPrimer über Telnet müssen Sie eine Verbindung zwischen einem Telnet-Client und den Bereitstellungszielcomputern herstellen können. Hierfür müssen die in der Bereitstellungsanforderung angegebenen Root-/Administator-Anmeldeinformationen verwendet werden. Sie müssen auch in der Lage sein, über Manager-Zielcomputer einen FTP-Abrufvorgang durchzuführen und sich beim FTP-Server als anonymer Benutzer anzumelden.

Ändern von FTP-Serverdetails zur Verwendung mit Infrastructure Deployment

Die optionalen Details für den FTP-Server, auf dem Infrastructure Deployment-Pakete gespeichert werden, können nach Abschluss der Installation geändert werden, wenn Sie z. B. FTP-Pakete auf einen anderen Server verschieben möchten.

Um die optionalen Details auf einem Zielcomputer mit Windows zu ändern, führen Sie folgenden Befehl aus:

`\Program Files\CA\DSM\bin\dmdeploy.exe ftpinfo` *`FTP_server FTP_user FTP_password`*

FTP-Server

Gibt die Adresse des Host-Computers des FTP-Servers an.

FTP-Benutzer

Gibt den Benutzer an, der eine Verbindung zum FTP-Server herstellt.

FTP-Kennwort

Gibt das dem FTP-Benutzer zugeordnete Kennwort an.

Windows XP-Einstellung zum Aktivieren der Bereitstellung von Agenten

Zum Aktivieren der Bereitstellung von Agenten auf Zielcomputern, auf denen Firewall-Software ausgeführt wird (etwa Windows Firewall unter Windows XP Professional SP2) müssen Sie manuell folgende Aktionen ausführen:

1. Ändern Sie die Sicherheitsrichtlinie "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten" von "Nur Gast - lokale Benutzer authentifizieren sich als Gast" auf "Klassisch - lokale Benutzer authentifizieren sich als sie selbst" (gilt für Windows XP).

   Das klassische Modell lässt die genaue Kontrolle über den Zugriff auf Ressourcen zu und verhindert, dass Netzwerkanmeldungen, die lokale Konten verwenden, als Gastkonto behandelt werden, das normalerweise nur Lesezugriff auf Ressourcen erhält.

   Weitere Informationen finden Sie auf der Webseite "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten" der Windows-Produktdokumentation.

2. Konfigurieren Sie die folgenden Firewall-Einstellungen.

   - Ermöglicht die Datei- und Druckerfreigabe
   - Öffnen Sie UDP-Port 4104.
   - Öffnen Sie TCP-Port 135.

Kapitel 6: Hinweise zu Aktualisierungen und zur Migration

Dieses Kapitel enthält folgende Themen:

Unterstützte Upgrade-Pfade (siehe Seite 270)
Allgemeine Hinweise (siehe Seite 270)
Aktualisierungsvorgang (siehe Seite 274)
Wichtige Hinweise zur Aktualisierung (siehe Seite 275)
Phase 1: Upgrade des DSM-Enterprise-Managers (siehe Seite 276)
Phase 2: Upgrade des DSM-Domänen-Managers (siehe Seite 277)
Phase 3: Upgrade der DSM-Scalability-Server (siehe Seite 278)
Phase 4: Upgrade der DSM-Agenten (siehe Seite 279)
Upgrade von Agenten mit Hilfe der Installations-DVD (siehe Seite 280)
Aktualisieren von Windows-Agenten mit Hilfe von Infrastructure Deployment und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins (siehe Seite 280)
Upgrade von Windows-Agenten mit Hilfe von Infrastructure Deployment und des individuellen Agenten-Plug-ins (siehe Seite 281)
Upgrade von Linux- oder MacIntel-Agenten mithilfe von Infrastructure Deployment und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins (siehe Seite 282)
Upgrade von Linux- oder MacIntel-Agenten mithilfe von Infrastructure Deployment und des individuellen Agenten-Plug-in-Pakets (siehe Seite 282)
Upgrade von Linux- oder MacIntel-Agenten mithilfe von Software Delivery und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins (siehe Seite 283)
Upgrade von Linux- oder MacIntel-Agenten mithilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets (siehe Seite 283)
Upgrade von Unix-Agenten mit Hilfe von Infrastructure Deployment und des Pakets "AM, SD Plug-in(s)". (siehe Seite 283)
Upgrade von UNIX-Agenten mit Hilfe von Infrastructure Deployment und des individuellen Agenten-Plug-ins (siehe Seite 284)
Aktualisieren von Windows-Agenten mit Hilfe von Software Delivery und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins (siehe Seite 284)
Upgrade von Windows-Agenten mit Hilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets (siehe Seite 285)
Upgrade von UNIX-Agenten mit Hilfe von V und des Pakets "AM, SD Plug-in(s)". (siehe Seite 285)
Upgrade von UNIX-Agenten mit Hilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets (siehe Seite 286)

Unterstützte Upgrade-Pfade

CA ITCM Version 12.8 unterstützt Aktualisierungen der folgenden Produkte und Versionen:

- Für Manager-Komponenten wird die Aktualisierung von den folgenden Versionen unterstützt:
  - CA ITCM 12.5
  - CA ITCM 12.5 SP1
  - CA ITCM 12.5 SP1 C1
- Für Scalability-Server und Agentenkomponenten wird das Upgrade unterstützt von:
  - CA ITCM 12.5
  - CA ITCM 12.5 SP1
  - CA ITCM 12.5 SP1 Feature Pack 1
  - CA ITCM 12.5 SP1 Kubuntu
  - CA ITCM 12.5 SP1 C1

Allgemeine Hinweise

Alle Aktualisierungen müssen mit identischen Sprachversionen durchgeführt werden. Beispielsweise können Sie eine deutsche auf eine deutsche Sprachversion von CA ITCM aktualisieren, nicht aber auf eine englische Sprachversion.

Hinweise zum CA ITCM-Komponenten-Upgrade

Wenn Sie das Upgrade von CA ITCM-Komponenten durchführen, beachten Sie folgende Hinweise:

- Die neuen Unterschriften, die vom CA ITCM Version 12.8-Scalability-Server zur Erkennung von Images der virtuellen Anwendung zur Verfügung gestellt werden, sind besonders gekennzeichnet und werden daher vom Legacy-Agenten ignoriert. Daher werden diese Signaturen und das Inventar der virtuellen Anwendungen nur von Agenten der Version 12.5 ordnungsgemäß bearbeitet.

Hinweise zu MDB

Es folgen die Hinweise zu MDB:

- CA ITCM Version 12.8 wird durch Microsoft SQL Server 2005 nicht als MDB unterstützt. Führen Sie das Upgrade des Datenbankmanagementsystems auf Microsoft SQL Server 2008 oder höher durch, bevor Sie das Upgrade auf CA ITCM Version 12.8 vornehmen.

Hinweise zu Aktualisierungen

Wenn Sie eine Aktualisierung auf Version 12.8 durchführen:

- CA ITCM aktualisiert nur die Komponenten, die in der vorherigen Version installiert wurden. Um die aktuellen Versionskomponenten oder zusätzliche Komponenten zu installieren, führen Sie das Installationsprogramm mit der Änderungsoption aus, und wählen Sie die zu installierenden Komponenten aus. Beispielsweise "Automatisierte Migration" und "Alarm-Collector".
- Wenn WAC mit SSL konfiguriert ist, bevor das Upgrade angewendet wird, stellen Sie sicher, dass Sie die Zertifikate in den JRE 1.7-Zertifikatsspeicher importieren, nachdem das Upgrade abgeschlossen wurde. Weitere Informationen finden Sie im Thema "Aktivieren von SSL für Webkonsole und Webservices" in der Webkonsolen-Hilfe.
- Wenn der CA Asset Management- oder CA Remote Control-Agent unter Windows über einen Software Delivery-Job aktualisiert wird, wird diesem Job automatisch das Software Delivery-Agentenpaket hinzugefügt. Der Software Delivery-Agent wird zuerst aktualisiert, gefolgt von den angeforderten Agents.
- Wenn Sie OSIM-IPS-Komponenten aktualisieren, müssen Sie sicherstellen, dass eine benutzerdefinierte Vorlage mit dem Namen "template.ini" gesichert wird, bevor die neueste Datei "template.ini" im OSIM-Installationsverzeichnis abgelegt wird. Extrahieren Sie beliebige benutzerdefinierte Änderungen aus der Sicherung der Datei "template.ini", und wenden Sie sie auf die neue Datei "template.ini" an. In künftigen Versionen soll CA ITCM erweiterbare Toolupdates enthalten, um die Anpassung der Datei "boiler template.ini" zu unterstützen.
- Damit die Plug-ins richtig funktionieren, führen Sie alle DSM-Plug-ins für die aktuelle Version aus.

Upgradeinformationen

Hinweis: Wenn Sie von CA ITCM r12.5 SP1 oder r12.5 SP1 C1 ein Upgrade vornehmen, wird CCS nicht aktualisiert. Die aktuelle Version enthält zusätzliche CCE-Patches, die erforderlich sind, um Windows Server 2012 und SQL Server 2012 zu unterstützen. Wenn Sie planen, ein Upgrade der Manager-Computer auf Windows Server 2012 oder SQL Server 2012 vorzunehmen, wenden Sie sich an den technischen Support von CA, um eine Liste mit den anzuwendenden Patches zu erhalten.

Während Sie ein Upgrade von R 12.5, R12.5 SP1 und R12.5 SP1C1 *auf CA ITCM Version 12.8 vornehmen, dürfen Sie "caf kill all" nicht vor dem Upgrade ausführen. Führen Sie ggf. "caf stop" aus.*

Hinweise zu FIPS

Es folgen die Hinweise zu FIPS:

- Wenn Sie ein Upgrade von vorhandenen CA ITCM-Komponenten durchführen, können Sie den FIPS-Modus nicht angeben; Upgrades erzwingen immer den Modus "FIPS-bevorzugt".
- Alle Komponenten, für die ein Upgrade durchgeführt wurde, verwenden den Modus "FIPS-bevorzugt", bis Sie sie ausdrücklich in den Modus "Nur-FIPS" ändern. Sie können in den Modus "Nur-FIPS" wechseln, wenn Sie alle Komponenten in der CA ITCM-Infrastruktur auf die aktuelle Version aktualisiert haben. Weitere Informationen über das Wechseln in die FIPS-Modi finden Sie im Abschnitt zu den Sicherheitsfunktionen.
- Nachdem Sie das Upgrade des Domänen-Managers und das Image Prepare Systems (IPS) durchgeführt haben, können Sie IPS verwenden, um das Upgrade des vorhandenen BS und der Boot-Images durchzuführen, mit dem Sie sie den FIPS-Standards anzupassen. Sie können sich dann registrieren und die migrierten Images auf die Boot-Server anwenden. Weitere Informationen zum Upgrade, zur Registrierung und zur Anwendung von BS-Images finden Sie im *BS-Installationsverwaltung - Administrationshandbuch*.

Weitere Informationen:

So wechseln Sie in "nur-FIPS" (siehe Seite 454)
So wechseln Sie in "FIPS-bevorzugt" (siehe Seite 455)

Hinweise zur Aktualisierung für OSIM

Führen Sie bei der Aktualisierung von ITCM vom R12.5 SP1 FP1 CentOS-Patch (R055831) oder von R12.5 SP1 FP1 C1 auf CA ITCM Version 12.8 folgende Schritte aus:

- Aktualisieren Sie das vorhandene Linux-basierte (LinuxPE) Boot-Image.
- Aktualisieren Sie die vorhandenen RHEL5.x- und RHEL6.x-LinuxPE-basierten BS-Images.
- Aktualisieren Sie vorhandene BS-Images (die zuvor durch WinPE und DOSx unterstützt wurden), die nun durch LinuxPE unterstützt werden. Nachdem Sie das vorhandene BS-Image aktualisiert haben, stellen Sie sicher, dass "sda", "sdb" dem Wert des Boot-Parameters "InstallDrive" entsprechen.
- Ändern Sie den Wert manuell in einen durch die BS-Images unterstützten.

Hinweis: Geben Sie den Boot-Parameter "InstallDrive" in Bezug auf die Verwendung der lokalen Festplatte für die BS-Installation an. Der Standardwert ist leer, und die erste verfügbare lokale Festplatte wird für die BS-Installation verwendet.

Eine Festplatte können Sie wie folgt hinzufügen:

- Fügen Sie die Festplatten über den DSM-Explorer, beispielsweise *sde, sdf*, für mehr als vier (4) Festplatten hinzu.
- Ändern Sie die Datei "OS.def" unter dem OSIM-IPS-Ordner (CA\DSM\osimips\os-template\camenu).

Im Folgenden finden Sie die neue Definition für den Boot-Parameter "InstallDrive" für Linux-basierte BS-Images:

```
[InstallDrive]

Type=MapListExt

Trans=yes

MaxLength=255

Comment=Disk to install the OS like sda or sdb or sdc. (Kommentar =
Festplatte zum Installieren des BS, beispielsweise sda oder sdb oder sdc.)

item=sda

item=sdb

item=sdc

item=sdd
```

Weitere Informationen hierzu finden Sie im BS-Installationsverwaltung - Administrationshandbuch.

Aktualisierungsvorgang

Das Upgrade von CA ITCM ist ein langwieriger Prozess, der von vielen externen Faktoren, wie beispielsweise fehlenden Systemressourcen und unerwartetem Leistungsabfall, beeinflusst wird. Vor jedem Upgrade, insbesondere vor dem Upgrade von Manager- und Serverkomponenten, sollten Sie eine vollständige Sicherung der vorhandenen Installation durchführen, um vor Datenverlusten geschützt zu sein.

Die Reihenfolge, in der Sie das Upgrade der Komponenten ausführen, ist wichtig. Diese Version von CA ITCM unterstützt eine streng hierarchisch strukturierte Aktualisierungsstrategie. Lesen Sie die unter den folgenden Phasen beschriebenen Schritte genau durch, bevor Sie fortfahren.

- Phase 1: Upgrade des DSM-Enterprise-Managers
- Phase 2: Upgrade des DSM-Domänen-Managers
- Phase 3: Upgrade der DSM-Scalability-Server
- Phase 4: Upgrade der DSM-Agenten

Die Konfiguration ist nach jedem Aktualisierungsschritt voll funktionsfähig, d. h., die aktualisierten Komponenten können mit noch nicht aktualisierten Komponenten kommunizieren.

Hinweis: Wenn Sie die zuvor auf einem Computer installierte CA ITCM-Software über die CA ITCM-Installations-DVD aktualisieren, werden alle auf diesem Computer installierten CA ITCM-Komponenten aktualisiert.

Hinweis: Wenn Sie Ihre vorhandene Installation von einer anderen Installationsquelle als der bei der ursprünglichen Unicenter DSM-Installation verwendeten, beispielsweise einem DVD-Reader, aktualisieren möchten, schlägt die Upgrade-Installation möglicherweise mit dem MSI-Fehlercode 1602 fehl. Um dieses Problem zu vermeiden, sollten Sie Ihre Installation so konfigurieren, dass dieselbe Quelle bzw. derselbe Datenträger, der auch schon für die ursprüngliche Installation verwendet wurde, eingesetzt wird.

Wichtige Hinweise zur Aktualisierung

- Sie können die Sprache für eine vorhandene Installation während eines Upgrade nicht ändern. Wenn Sie, z. B. in der Antwortdatei für eine unbeaufsichtigte Aktualisierung, eine andere Sprach-ID angeben, wird die Aktualisierung abgebrochen.
- Navigieren Sie im DSM-Explorer zu "Systemsteuerung, Konfiguration, Konfigurationsrichtlinie, Richtlinienname, DSM, Manager, Infrastructure Deployment", und stellen Sie sicher, dass der Wert des Parameters "Primer immer bereitstellen" auf "False" gesetzt ist.

  Wenn der Wert des Parameters auf "False" gesetzt ist, führt der Manager ein Upgrade von DMprimer nur auf jenen Zielcomputern durch, deren Version von DMprimer niedriger als die des Managers ist. Wenn Sie den Parameter auf "True" setzen, führt der Manager ungeachtet der Versionen von DMprimer ein Upgrade auf den Zielcomputern durch.
- Beim Upgrade werden die Zertifikate nicht aktualisiert, um auf dem Computer möglicherweise bereits vorhandene benutzerdefinierte Zertifikate zu schützen. Wenn ein Master-Image für die Verwendung neuer benutzerdefinierter Zertifikate aktualisiert wurde, werden diese bei der Installation in den Ordner "bin" kopiert, jedoch nicht auf den Zertifikatspeicher angewendet.

  Benutzerdefinierte Zertifikate müssen bei den Erstinstallationen oder manuell nach einer Aktualisierung angewendet werden. Die für den Import neuer Zertifikate erforderlichen Befehle werden im Abschnitt "Authentifizierung" (siehe Seite 403) des Kapitels "Sicherheitsfunktionen" erläutert.

Weitere Informationen:

So wechseln Sie in "nur-FIPS" (siehe Seite 454)
So wechseln Sie in "FIPS-bevorzugt" (siehe Seite 455)

Phase 1: Upgrade des DSM-Enterprise-Managers

In Phase 1 der Aktualisierung aktualisieren Sie den DSM-Enterprise-Manager. Enterprise-Manager werden normalerweise nur in sehr großen Unternehmen oder Unternehmen mit sehr stark verteilten Umgebungen installiert. Wurde zuvor bei Ihnen kein DSM-Enterprise-Manager installiert, gehen Sie direkt zu Phase2.

Gehen Sie folgendermaßen vor, um den Enterprise-Manager zu aktualisieren:

1. Beenden Sie alle Dienste und Anwendungen, die möglicherweise über eine Verbindung mit der DSM-Enterprise-MDB verfügen.

   In einer reinen CA ITCM-Implementierung gehören hierzu der DSM-Enterprise-Manager selbst, Remote-Engines für die Enterprises und Domänen sowie aktive Instanzen des DSM-Reporters. Wenn in Ihrem Netzwerk andere CA-Anwendungen oder Produkte von Drittanbietern installiert sind, die auch auf die MDB zugreifen und somit auch über eine aktive Verbindung verfügen können, müssen diese auch beendet werden.

2. Aktualisieren Sie die MDB mit Hilfe der DVD (falls möglich).

   Wenn die MDB auf einem vom DSM-Enterprise-Manager entfernten Computer installiert ist, führen Sie das Upgrade der MDB mit Hilfe der CA ITCM-DVD durch. Wählen Sie "MDB installieren" oder "CCS einschließlich MDB installieren" aus.

3. Führen Sie das Upgrade des DSM-Enterprise-Manager mit Hilfe der DVD durch.

4. Führen Sie das Upgrade aller DSM-Enterprise-Engines mit Hilfe der DVD durch (falls nötig).

   Wenn auf Remote-Computern zuvor bereits Enterprise-Engines installiert waren, aktualisieren Sie diese jetzt mit Hilfe der CA ITCM-DVD.

5. Führen Sie das Upgrade aller DSM-Explorer bzw. DSM-Reporter mittels der DVD oder des Software Delivery-Pakets durch (falls nötig).

   Für alle eigenständigen Instanzen von DSM-Explorer, DSM-Reporter, Webdiensten oder Webkonsole, die im Verbindung mit dem DSM-Enterprise-Manager stehen und für die in den vorangegangenen Schritten kein Upgrade durchgeführt wurde, sollten dies nun getan werden. Für Instanzen, die auf Computern mit einem DSM-Scalability-Server oder einem DSM-Agenten installiert sind, sollten nach Phase 3 bzw. Phase 4 ein Upgrade ausgeführt werden.

Hinweis: CA ITCM Version 12.8 ist nur mit CA Asset Intelligence Version 12.8 oder CA Patch Manager Version 12.8 kompatibel. Wenn Sie ein Upgrade auf CA ITCM Version 12.8 durchführen, müssen Sie auch Upgrades für CA Asset Intelligence oder CA Patch Manager auf Version 12.8 durchführen.

Hinweis: Wenn Sie von CA ITCM r12.5 SP1 oder r12.5 SP1 C1 ein Upgrade vornehmen, wird CCS nicht aktualisiert. Die aktuelle Version enthält zusätzliche CCE-Patches, die erforderlich sind, um Windows Server 2012 und SQL Server 2012 zu unterstützen. Wenn Sie planen, ein Upgrade der Manager-Computer auf Windows Server 2012 oder SQL Server 2012 vorzunehmen, wenden Sie sich an den technischen Support von CA, um eine Liste mit den anzuwendenden Patches zu erhalten.

Während Sie ein Upgrade von R 12.5, R12.5 SP1 und R12.5 SP1C1 *auf CA ITCM Version 12.8 vornehmen, dürfen Sie "caf kill all" nicht vor dem Upgrade ausführen. Führen Sie ggf. "caf stop" aus.*

Phase 2: Upgrade des DSM-Domänen-Managers

In Phase 2 des CA ITCM-Upgrades aktualisieren Sie den DSM-Domänen-Manager.

Gehen Sie folgendermaßen vor, um den DSM-Domänen-Manager zu aktualisieren:

1. Beenden Sie alle Dienste und Anwendungen, die möglicherweise über eine Verbindung mit der DSM-Domänen-MDB verfügen.

   In einer reinen CA ITCM-Implementierung gehören hierzu der DSM-Domänen-Manager selbst, Remote-Engines für die Enterprise und Domänen, sowie aktive Instanzen des DSM-Reporters (für diese Domäne und für den übergeordneten Enterprise-Manager). Wenn in Ihrem Netzwerk andere CA-Anwendungen oder Produkte von Drittanbietern installiert sind, die auch auf die MDB zugreifen und somit auch über eine aktive Verbindung verfügen können, müssen diese auch beendet werden.

2. Führen Sie das Upgrade der MDB mit Hilfe der CA ITCM-Installations-DVD durch (falls nötig).

   Wenn die MDB auf einem vom DSM-Domänenmanager entfernten Computer installiert ist, führen Sie das Upgrade der MDB mit Hilfe der Installations-DVD durch. Wählen Sie "MDB installieren" oder "CCS einschließlich MDB installieren" aus.

3. Führen Sie das Upgrade des DSM-Domänenmanagers mit Hilfe der DVD durch.

4. Führen Sie das Upgrade aller DSM-Domänen-Engines mit Hilfe der DVD durch (falls nötig).

   Wenn auf Remote-Computern zuvor bereits DSM-Engines auf Domänenebene installiert waren, führen Sie deren Upgrade jetzt mit Hilfe der Installations-DVD durch.

5. Führen Sie das Upgrade aller DSM-Explorer bzw. DSM-Reporter mittels der Installations-DVD oder des Software Delivery-Pakets durch (falls nötig).

   Für alle eigenständigen Instanzen von DSM-Explorer, DSM-Reporter, Webdiensten oder Webkonsole, die im Verbindung mit dem DSM-Domänenmanager stehen und für die in den vorangegangenen Schritten kein Upgrade durchgeführt wurde, sollten dies nun getan werden. Für Instanzen, die auf Computern mit einem DSM-Scalability-Server oder einem DSM-Agenten installiert sind, sollten nach Phase 3 bzw. Phase 4 ein Upgrade ausgeführt werden.

Hinweis: CA ITCM Version 12.8 ist nur mit CA Asset Intelligence Version 12.8 oder CA Patch Manager Version 12.8 kompatibel. Wenn Sie ein Upgrade auf CA ITCM Version 12.8 durchführen, müssen Sie auch Upgrades für CA Asset Intelligence oder CA Patch Manager auf Version 12.8 durchführen.

Hinweis: Wenn Sie von CA ITCM r12.5 SP1 oder r12.5 SP1 C1 ein Upgrade vornehmen, wird CCS nicht aktualisiert. Die aktuelle Version enthält zusätzliche CCE-Patches, die erforderlich sind, um Windows Server 2012 und SQL Server 2012 zu unterstützen. Wenn Sie planen, ein Upgrade der Manager-Computer auf Windows Server 2012 oder SQL Server 2012 vorzunehmen, wenden Sie sich an den technischen Support von CA, um eine Liste mit den anzuwendenden Patches zu erhalten.

Während Sie ein Upgrade von R 12.5, R12.5 SP1 und R12.5 SP1C1 *auf CA ITCM Version 12.8 vornehmen, dürfen Sie "caf kill all" nicht vor dem Upgrade ausführen. Führen Sie ggf. "caf stop" aus.*

Phase 3: Upgrade der DSM-Scalability-Server

Upgrades der DSM-Scalability-Server können mit einer der folgenden drei Methoden durchgeführt werden:

- Verwenden der CA ITCM-Installations-DVD
- Verwenden von Software Delivery-Paketen für Scalability-Server
- Verwenden von Infrastructure Deployment (DMDeploy) für Scalability-Server

Um die Scalability-Server mit Hilfe der Installations-DVD zu aktualisieren, legen Sie die DVD in den entsprechenden Computer ein, und starten Sie den interaktiven Installationsassistenten.

Um das Upgrade von Scalability-Servern mit Hilfe von Software Delivery-Paketen durchzuführen, erstellen Sie einen Software Delivery-Bereitstellungsjob, der das DSM-Scalability-Server-Paket enthält, und planen Sie die Ausführung des Software Delivery-Jobs auf den Scalability-Server-Computern.

Um Windows-Scalability-Server mit Hilfe von Infrastructure Deployment (DMDeploy) zu aktualisieren, stellen Sie das neue Scalability-Server-Paket auf den Scalability-Server-Computern bereit. Dadurch werden sowohl der Scalability-Server selbst als auch der Agent und alle bereits installierten Agenten-Plug-ins aktualisiert. Um das Installationsprogramm zur Aktualisierung der Agenten-Plug-ins anzuweisen, müssen Sie die folgenden Parameter in das Feld für die zusätzlichen Windows-Installationsoptionen des Infrastructure Deployment-Assistenten eingeben.

REINSTALL=ALL REINSTALLMODE=vomus

Um Linux-Scalability-Server mit Infrastructure Deployment (DMDeploy) zu aktualisieren, müssen Sie das neue Scalability-Server-Paket auf den Scalability-Server-Computern bereitstellen. Dadurch werden sowohl der Scalability-Server selbst als auch der Agent und alle bereits installierten Agenten-Plug-ins aktualisiert.

Phase 4: Upgrade der DSM-Agenten

Zum Upgrade der DSM-Agenten stehen verschiedene Methoden zur Auswahl, die im Folgenden beschrieben werden. Lesen Sie die folgenden Methoden sorgfältig durch, und wählen Sie eine geeignete aus. Im Anschluss an diese Liste finden Sie detaillierte Aktualisierungsanweisungen.

- Verwenden der CA ITCM-Installations-DVD für Windows-, Linux-, MacIntel- und UNIX-Computer.
- Verwenden von Infrastructure Deployment (DMDeploy) für Computer mit Windows-, Linux- und MacIntel-Agenten und des Pakets "AM, RC, SD plugin(s)" (für alle Agenten-Plug-ins).

  Wenn auf den Agent-Computern bereits alle Agenten-Plug-ins installiert sind, können Sie zur Aktualisierung das Paket für alle Agenten-Plug-ins verwenden. Ist dies nicht der Fall, können Sie dieses Paket dennoch verwenden, müssen jedoch beachten, dass unter Windows alle nicht installierten Plug-ins hinzugefügt werden.
- Verwenden von Infrastructure Deployment für Computer mit UNIX-Agenten und des Pakets "AM, SD Plug-in(s)" für alle Agenten-Plug-ins
- Verwenden von Infrastructure Deployment für Computer mit Windows-, Linux-, MacIntel- und UNIX-Agenten und der individuellen Agenten-Plug-in-Pakete.
- Mit Hilfe von Infrastructure Deployment können Sie auf einem eigenständigen RC-Agenten eine Aktualisierung durchführen.
- Verwenden von Software Delivery für Computer mit Windows-, Linux- und MacIntel-Agenten und des Pakets "AM, RC, SD plugin(s)" (für alle Agenten-Plug-ins) oder der individuellen Agenten-Plug-in-Pakete.

  Wenn auf den Agent-Computern bereits alle Agenten-Plug-ins installiert sind, können Sie zur Aktualisierung das Paket für alle Agenten-Plug-ins verwenden. Ist dies nicht der Fall, können Sie dieses Paket dennoch verwenden, müssen jedoch beachten, dass unter Windows alle nicht installierten Plug-ins hinzugefügt werden.

- Verwenden von Software Delivery für Computer mit UNIX-Agenten und des Pakets "AM, SD Plug-in(s)" für alle Agenten-Plug-ins

  Hinweis: Wenn Sie eine Aktualisierung von DSM-Agenten durchführen, müssen Sie die folgenden Patches anwenden, bevor Sie die Aktualisierung mit Software Delivery durchführen.

  - AIX: RO01350
  - HP: RO01319
  - SUN: RO01315

Upgrade von Agenten mit Hilfe der Installations-DVD

Um DSM-Agenten mit Hilfe der Installations-DVD zu aktualisieren, legen Sie die DVD in den Agent-Computer ein, und verwenden Sie den interaktiven Installationsassistenten.

Aktualisieren von Windows-Agenten mit Hilfe von Infrastructure Deployment und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins

Wenn auf den Agent-Computern bereits alle Agenten-Plug-in installiert sind, können Sie zur Aktualisierung das Paket für alle Agenten-Plug-ins verwenden. Das Paket für alle Agenten-Plug-ins aktualisiert die AM-, RC- und SD-Plug-ins, aber nicht das DTS-Plug-in. Aktualisieren Sie das DTS-Plug-in mit dem DTS-Paket.

Hinweis: Mit dem Paket für alle Agenten-Plug-ins unter Windows werden auch Plug-ins installiert, die zuvor noch nicht installiert waren, mit Ausnahme des STS-Plug-ins.

Um DSM-Agenten mit Hilfe von Infrastructure Deployment für Computer mit Windows-Agenten und des Pakets für alle Agenten-Plug-ins zu aktualisieren, stellen Sie das Paket "AM, RC, SD plugin(s)" auf den Agent-Computern bereit.

Um das Installationsprogramm zur Aktualisierung anzuweisen, müssen Sie die folgenden Parameter in das Feld für die zusätzlichen Windows-Installationsoptionen des Infrastructure Deployment-Assistenten eingeben.

REINSTALL=ALL REINSTALLMODE=vomus

Upgrade von Windows-Agenten mit Hilfe von Infrastructure Deployment und des individuellen Agenten-Plug-ins

Gehen Sie folgendermaßen vor, um ein Upgrade des DSM-Agenten mit Hilfe von Infrastructure Deployment für Computer mit Windows-Agenten und den individuellen Agenten-Plug-in-Paketen durchzuführen:

- Stellen Sie das Paket des DSM Remote Control-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Remote Control-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

  Um das Installationsprogramm zur Aktualisierung des Agenten-Plug-ins anzuweisen, müssen Sie die folgenden Parameter in das Feld für die zusätzlichen Windows-Installationsoptionen des Infrastructure Bereitstellungsassistenten eingeben.

  REINSTALL=ALL REINSTALLMODE=vomus

- Stellen Sie das Paket des DSM-Software Delivery-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Software Delivery-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

  Um das Installationsprogramm zur Aktualisierung des Agenten-Plug-ins anzuweisen, müssen Sie die folgenden Parameter in das Feld für die zusätzlichen Windows-Installationsoptionen des Infrastructure Bereitstellungsassistenten eingeben.

  REINSTALL=ALL REINSTALLMODE=vomus

- Stellen Sie das Paket des DSM Asset Management-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Asset Management-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

  Um das Installationsprogramm zur Aktualisierung des Agenten-Plug-ins anzuweisen, müssen Sie die folgenden Parameter in das Feld für die zusätzlichen Windows-Installationsoptionen des Infrastructure Bereitstellungsassistenten eingeben.

  REINSTALL=ALL REINSTALLMODE=vomus

- Stellen Sie das Paket des DSM-Basisinventar-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Basisinventar-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

  Um das Installationsprogramm zur Aktualisierung des Agenten-Plug-ins anzuweisen, müssen Sie die folgenden Parameter in das Feld für die zusätzlichen Windows-Installationsoptionen des Infrastructure Bereitstellungsassistenten eingeben.

  REINSTALL=ALL REINSTALLMODE=vomus

Upgrade von Linux- oder MacIntel-Agenten mithilfe von Infrastructure Deployment und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins

Um DSM-Agenten mithilfe von Infrastructure Deployment für Computer mit Linux- oder MacIntel-Agenten und des Pakets für alle Agenten-Plug-ins zu aktualisieren, stellen Sie das Paket "AM, RC, SD plugin(s)" auf den Agent-Computern bereit.

Standardmäßig aktualisiert das Paket für alle Agenten-Plug-ins die früheren Versionen der installierten Agenten-Plug-ins. Es werden keine neuen Plug-in hinzugefügt.

Upgrade von Linux- oder MacIntel-Agenten mithilfe von Infrastructure Deployment und des individuellen Agenten-Plug-in-Pakets

Gehen Sie folgendermaßen vor, um ein Upgrade des DSM-Agenten mithilfe von Infrastructure Deployment für Computer mit Linux- oder MacIntel-Agenten und den individuellen Agenten-Plug-in-Paketen durchzuführen:

- Stellen Sie das Paket des DSM Remote Control-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Remote Control-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

- Stellen Sie das Paket des DSM-Software Delivery-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Software Delivery-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

- Stellen Sie das Paket des DSM Asset Management-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Asset Management-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen

- Stellen Sie das Paket des DSM-Basisinventar-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Basisinventar-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

Upgrade von Linux- oder MacIntel-Agenten mithilfe von Software Delivery und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins

Gehen Sie folgendermaßen vor, um ein Upgrade der DSM-Agenten mithilfe von Software Delivery für Computer mit Linux- oder MacIntel-Agenten und des Pakets für alle Agenten-Plug-ins durchzuführen:

- Erstellen Sie einen Software Delivery-Bereitstellungsjob, der das Paket für "alle Agenten-Plug-ins" enthält.
- Planen Sie die Ausführung des Software Delivery-Jobs auf den Agent-Computern.

  Standardmäßig aktualisiert das Paket für alle Agenten-Plug-ins die früheren Versionen der installierten Agenten-Plug-ins. Es werden keine neuen Plug-in hinzugefügt.

Upgrade von Linux- oder MacIntel-Agenten mithilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets

Gehen Sie folgendermaßen vor, um ein Upgrade des DSM-Agenten mithilfe von Software Delivery für Computer mit Linux- oder MacIntel-Agenten und den individuellen Agenten-Plug-in-Paketen durchzuführen:

- Erstellen Sie einen Software Delivery-Bereitstellungsjob, der mindestens den DSM-Agenten und das Software Delivery-Agenten-Plug-in enthält.

  Wenn auf den Agent-Computern auch frühere Versionen anderer DSM-Agenten-Plug-ins installiert wurden, müssen die Jobs auch diese abdecken.
- Planen Sie die Ausführung des Software Delivery-Jobs auf den Agent-Computern.

Upgrade von Unix-Agenten mit Hilfe von Infrastructure Deployment und des Pakets "AM, SD Plug-in(s)".

Um DSM-Agenten mit Hilfe von Infrastructure Deployment für Computer mit UNIX-Agenten und des Pakets für alle Agenten-Plug-ins zu aktualisieren, stellen Sie das Paket "AM, SD Plug-in(s)" auf den Agent-Computern bereit.

Standardmäßig aktualisiert das Paket für alle Agenten-Plug-ins die früheren Versionen der installierten Agenten-Plug-ins. Es werden keine neuen Plug-ins hinzugefügt.

Upgrade von UNIX-Agenten mit Hilfe von Infrastructure Deployment und des individuellen Agenten-Plug-ins

Gehen Sie folgendermaßen vor, um ein Upgrade des DSM-Agenten mit Hilfe von Infrastructure Deployment für Computer mit UNIX-Agenten und den individuellen Agenten-Plug-in-Paketen durchzuführen:

- Stellen Sie das Paket des DSM-Software Delivery-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Software Delivery-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

- Stellen Sie das Paket des DSM Asset Management-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Asset Management-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen

- Stellen Sie das Paket des DSM-Basisinventar-Agenten-Plug-ins auf dem Agent-Computer bereit (falls nötig).

  Wenn eine frühere Version des Basisinventar-Agenten-Plug-ins auf dem Agent-Computer installiert ist, sollten Sie die neue Version des Plug-ins bereitstellen.

Aktualisieren von Windows-Agenten mit Hilfe von Software Delivery und des Pakets "AM, RC, SD plugin(s)" für alle Agenten-Plug-ins

Wenn auf den Agent-Computern bereits alle Agenten-Plug-ins installiert sind, können Sie zur Aktualisierung das Paket für alle Agenten-Plug-ins verwenden. Ist dies nicht der Fall, können Sie dieses Paket dennoch verwenden, müssen jedoch beachten, dass unter Windows alle nicht installierten Plug-ins hinzugefügt werden.

Gehen Sie folgendermaßen vor, um ein Upgrade von DSM-Agenten mit Hilfe von Software Delivery für Computer mit Windows-Agenten und des Pakets für alle Agenten-Plug-ins durchzuführen:

- Erstellen Sie einen Software Delivery-Bereitstellungsjob, der das Paket für alle Agenten-Plug-ins enthält.
- Planen Sie die Ausführung des Software Delivery-Jobs auf den Agent-Computern.

Upgrade von Windows-Agenten mit Hilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets

Gehen Sie folgendermaßen vor, um ein Upgrade des DSM-Agenten mit Hilfe von Software Delivery für Computer mit Windows-Agenten und den individuellen Agenten-Plug-in-Paketen durchzuführen:

- Erstellen Sie einen Software Delivery-Bereitstellungsjob, der mindestens den DSM-Agenten und das Software Delivery-Agenten-Plug-in enthält.

  Wenn auf den Agent-Computern auch frühere Versionen anderer DSM-Agenten-Plug-ins installiert wurden, müssen die Jobs auch diese abdecken.
- Planen Sie die Ausführung des Software Delivery-Jobs auf den Agent-Computern.

Upgrade von UNIX-Agenten mit Hilfe von V und des Pakets "AM, SD Plug-in(s)".

Hinweis: Wenn Sie ein Upgrade von r11.1 UNIX-Agenten durchführen, müssen Sie die folgenden Patches anwenden, bevor Sie das Upgrade mit Software Delivery durchführen.

- AIX: RO01350
- HP: RO01319
- SUN: RO01315

Gehen Sie folgendermaßen vor, um ein Upgrade von DSM-Agenten mit Hilfe von Software Delivery für Computer mit UNIX-Agenten und des Pakets für alle Agenten-Plug-ins durchzuführen:

- Erstellen Sie einen Software Delivery-Bereitstellungsjob, der das Paket für "alle Agenten-Plug-ins" enthält.
- Planen Sie die Ausführung des Software Delivery-Jobs auf den Agent-Computern.

  Standardmäßig führt das Paket für alle Agenten-Plug-ins Upgrades früherer Versionen der installierten Agenten-Plug-ins durch. Es werden keine neuen Plug-in hinzugefügt.

Upgrade von UNIX-Agenten mit Hilfe von Software Delivery und des individuellen Agenten-Plug-in-Pakets

Hinweis: Wenn Sie ein Upgrade von r11.1 UNIX-Agenten durchführen, müssen Sie die folgenden Patches anwenden, bevor Sie das Upgrade mit Software Delivery durchführen.

- AIX: RO01350
- HP: RO01319
- SUN: RO01315

Gehen Sie folgendermaßen vor, um ein Upgrade des DSM-Agenten mit Hilfe von Software Delivery für Computer mit UNIX-Agenten und den individuellen Agenten-Plug-in-Paketen durchzuführen:

- Erstellen Sie einen Software Delivery-Bereitstellungsjob, der mindestens den DSM-Agenten und das Software Delivery-Agenten-Plug-in enthält.

  Wenn auf den Agent-Computern auch frühere Versionen anderer DSM-Agenten-Plug-ins installiert wurden, müssen die Jobs auch diese abdecken.
- Planen Sie die Ausführung des Software Delivery-Jobs auf den Agent-Computern.

Kapitel 7: CA ITCM-Connector für CA Catalyst

CA Catalyst -Connectors zeigen Produktdaten für die Produkte, die sie verwenden, z. B. CA Spectrum Service Assurance und CA IT Process Automation Manager, für Visualisierungs-, Analyse- und Managementzwecke in einem eindeutigen, heterogenen Kontext an.

Hinweis: Sie können den CA ITCM-Connector mit einem vorhandenen Domain Manager oder Scalability-Server nur unter Windows-Betriebssystemen installieren.

Der CA ITCM-Connector unterstützt SSA 3.2.0. Der CA ITCM-Connector stellt eine Verbindung mit dem DSM-Domänen-Manager oder einem eigenständigen mit einem Domänen-Manager registrierten Scalability-Server her, um CA ITCM-Daten für die Verwendung durch Produkte anzuzeigen, die die CA Catalyst-Infrastruktur nutzen. Die Integration der CA ITCM-Daten mit den Produkten, die sie verwenden, z. B. [set the varname value at the book level], ermöglicht die Abstimmung und Korrelation von Entitätseigenschaften mit vorhandenen Configuration Items (CIs). Durch die Integration können Sie die Daten auch in einem anderen, breiteren Unternehmensdienstkontext auswerten.

Hinweis: CA ITCM-Connector 3.2.0 unterstützt nur Northbound auf SOI 3.2.0.

Bei vorhandener CA Catalyst-Connectorintegration steht ein CA ITCM-Connector pro Domäne zur Verfügung. Der CA ITCM-Connector wird mit dem Domain Manager mithilfe der folgenden CA ITCM-Komponenten oder -Funktionen verbunden:

- CA ITCM-Webservices

  Mit CA ITCM-Webservices werden Informationen zu den CIs abgerufen, die im CA Catalyst-Connector veröffentlicht werden sollen.

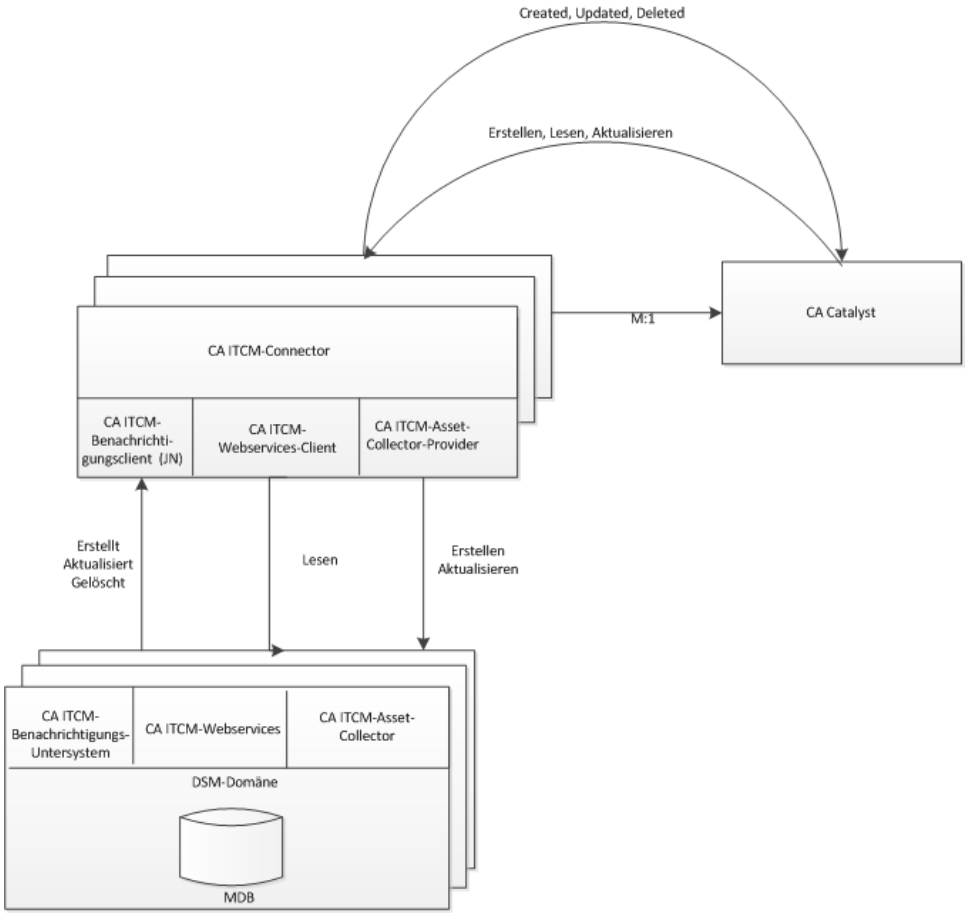
- CA ITCM-Subsystem für Ereignisbenachrichtigungen

  Ereignisse in Bezug auf Updates für veröffentlichte CIs werden über das CA ITCM-Subsystem für Ereignisbenachrichtigungen empfangen.

- Asset Collector

  Die Asset Collector-Komponente wird während CA Spectrum SA-Abonnierungsvorgängen für Computer-CI-Daten verwendet. Die Asset Collector-Dateien helfen bei der Verschiebung der eingehenden Erstellungsdaten und Aktualisierungsdaten vom Connector zur CA ITCM-MDB.

In der folgenden Grafik wird die CA ITCM-CA Catalyst-Connectorintegration zusammengefasst:



Hinweis: Allgemeine Informationen zur CA Catalyst-Infrastruktur und den zugehörigen Connectors, Informationen, die sich auf alle Connectors beziehen, und Informationen zu benutzerdefinierten Connector-Integrationen finden Sie im *Connector-Handbuch*, das mit CA Spectrum SA geliefert wird. Vollständige Informationen zum Installieren, Konfigurieren und Verwenden des CA ITCM-Connectors finden Sie im Handbuch zum *CA IT Client Manager Connector*, das ebenfalls mit CA Spectrum SA geliefert wird.

Kapitel 8: Desktop-Virtualisierung

Dieser Abschnitt umfasst die Szenarien in Bezug auf die Verwendung der Unterstützung der Desktop-Virtualisierungsfunktion. Mithilfe von CA ITCM können Sie Ihre virtuelle Desktop-Infrastruktur auf VMware View und Citrix XenDesktop verwalten. Mit CA ITCM ist Folgendes möglich:

- Sie können das Golden Template, vDisks und virtuelle Desktops über den DSM-Explorer verwalten.
- Sie können die automatische Neuinstallation der auf virtuellen Desktops installierten Software konfigurieren, ohne dass sich dies auf Ihre Änderungen nach dem Neustart oder nach einer Desktop-Aktualisierung mit einer neuen Version des Golden Templates auswirkt.

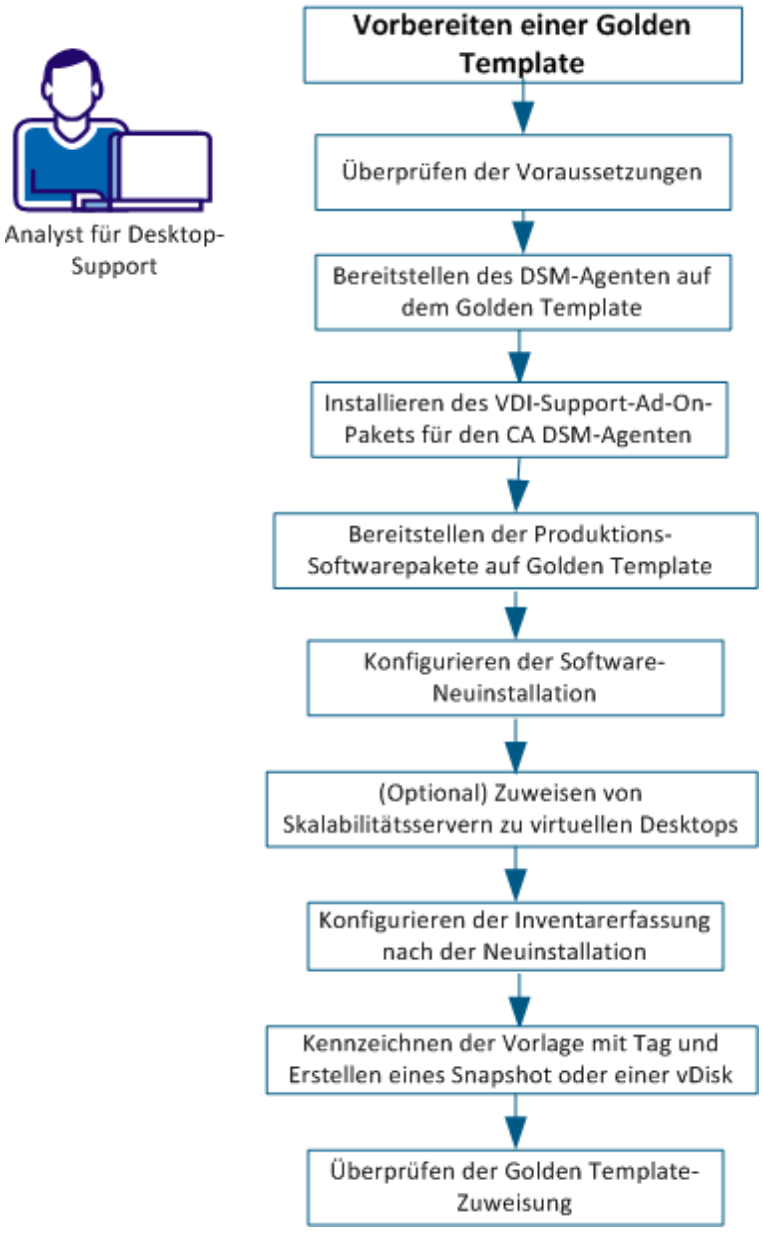
  Beispielsweise geht Software, die auf einem Standardmodus-vDisk-basierten virtuellen Desktop installiert ist, nach Ihrer Abmeldung verloren. Sie können CA ITCM so konfigurieren, dass diese Software bei Ihrer nächsten Anmeldung automatisch neu installiert wird.
- Enthält ein neues virtuelles Desktop-Identifizierungs- und Registrierungsschema, eine verbesserte Asset-Registrierungsgeschwindigkeit und Abfragen und Berichte.

  Hinweis: Die Verwaltung von Benutzerprofilen, Benutzerdaten, der Benutzerpersönlichkeit oder der Desktop-Konfiguration wird von dieser Version nicht unterstützt. Von Microsoft entwickelte Methoden wie das Roaming von Benutzerprofilen und die Ordnerumleitung handhaben stattdessen diese Tasks. Weitere Informationen finden Sie in der entsprechenden Microsoft-Dokumentation.

Vorbereiten von Golden Templates

Als ein Desktop-Support-Analyst müssen Sie Golden Templates vorbereiten, um Ihre virtuelle Desktop-Lösung in CA ITCM zu integrieren. Diese Integration hilft Ihnen dabei, Golden Templates, VMware View-Klone, Citrix PVS gestreamte virtuelle Desktops oder MCS-basierte virtuelle Desktops von CA ITCM zu verwalten.

Das folgende Diagramm veranschaulicht die Schritte für das Vorbereiten eines Golden Template:


Vorbereiten einer Golden Template
Analyst für Desktop-Support
Überprüfen der Voraussetzungen
Bereitstellen des DSM-Agenten auf dem Golden Template
Installieren des VDI-Support-Ad-On-Pakets für den CA DSM-Agenten
Bereitstellen der Produktions-Softwarepakete auf Golden Template
Konfigurieren der Software-Neuinstallation
(Optional) Zuweisen von Skalabilitätsservern zu virtuellen Desktops
Konfigurieren der Inventarerfassung nach der Neuinstallation
Kennzeichnen der Vorlage mit Tag und Erstellen eines Snapshot oder einer vDisk
Überprüfen der Golden Template-Zuweisung

Die Vorbereitung eines Golden Template umfasst die folgenden Tasks:

1. Überprüfen der Voraussetzungen (siehe Seite 291)
2. Bereitstellen des DSM-Agenten im Golden Template (siehe Seite 293)
3. Installieren des CA DSM-Agent VDI-Support-Add-on-Pakets (siehe Seite 293)
4. Bereitstellen von Produktions-Softwarepaketen im Golden Template (siehe Seite 294)
5. Konfigurieren der Software-Neuinstallation (siehe Seite 295)
6. Kennzeichnen der Vorlage und Erstellen eines Snapshots oder vDisks (siehe Seite 307)
7. (Optional) Zuweisen von Scalability-Servern zu virtuellen Desktops (siehe Seite 305)
8. Konfigurieren der Inventarerfassung bei Software-Neuinstallation (siehe Seite 306)
9. Überprüfen der Golden Template-Zuweisung (siehe Seite 308)

Überprüfen der Voraussetzungen

Um ein Golden Template vorzubereiten, überprüfen Sie die folgenden Voraussetzungen:

- Überprüfen Sie, ob der virtuelle Desktop-Agent auf dem Golden Template-Computer installiert ist.

  Hinweis: Ein umfassendes Wissen zu virtuellen Desktop-Lösungen wie VMware View und Citrix XenDesktop ist erforderlich, um die Integration mit CA ITCM zu implementieren.
- Überprüfen Sie, dass das Citrix PVS-Zielgerät auf dem Golden Template-Computer installiert ist, wenn Sie Citrix vDisk-basierte virtuelle Desktops erstellen möchten.
- (Nur für Citrix XenDesktop 7) Stellen Sie sicher, dass .Net 3.5 verfügbar ist.

Bereitstellen des DSM-Agenten im Golden Template

CA ITCM gibt unterschiedliche DSM-Agent-Pakete je nach den benötigten Funktionen an. Mindestens benötigen Sie den DSM Common Agent und den Software Delivery-Agent (CA DSM-Agent + Software Delivery-Plug-in). Wenn Sie die vollständige Funktionalität wünschen, stellen Sie das CA DSM-Agent + AM, RC, SD-Plug-in-Paket bereit.

Hinweis: DSM-Agent bezieht sich auf den DSM Common Agent und den Software Delivery-Agent (CA DSM-Agent + Software Delivery-Plug-in), nicht den vollständigen Agenten, wie erwähnt.

Die Bereitstellung des DSM-Agenten im Golden Template stellt sicher, dass der DSM-Agent auf den virtuellen Desktops verfügbar ist, die aus dem Golden Template erstellt werden. Das Golden Template und alle virtuellen Desktops werden als verwaltete Computer in CA ITCM hinzugefügt.

Gehen Sie wie folgt vor:

1. Navigieren Sie im DSM-Explorer zu "Systemsteuerung", "Bereitstellung", "Infrastructure Deployment-Assistent".
2. Folgen Sie den Anweisungen im Assistenten, und führen Sie die folgenden Tasks aus:
   - Wählen Sie ein Agentenpaket je nach den benötigten Funktionen aus.
   - Wählen Sie das Golden Template als Zielcomputer im Assistenten aus.
   - Geben Sie die IP-Adresse oder den voll qualifizierten Domänennamen (FQDN) des Scalability-Servers an, bei dem der bereitgestellte Agent registriert ist.
3. Klicken Sie auf "Fertig stellen".

   Ein Bereitstellungsjob wird unter "Systemsteuerung", "Bereitstellung", "Status des Bereitstellungsjobs" erstellt. Der Job wird an das Golden Template übergeben.
4. Überwachen Sie den Jobstatus im Knoten "Systemsteuerung", "Bereitstellung", "Status des Bereitstellungsjobs".

Nachdem die Bereitstellung erfolgreich verlaufen ist, wird der Agent automatisch beim Scalability-Server registriert. Nach der Registrierung wird das Golden Template im Domänen-Manager angezeigt.

Hinweis: Standardmäßig berichten das Golden Template und die virtuellen Desktops, die daraus bereitgestellt werden, an den gleichen Scalability-Server. Sie können einen anderen Scalability-Server für einen Bereich von virtuellen Desktops zuweisen, je nach dem Namensgebungsmuster der virtuellen Desktops. Weitere Informationen finden Sie unter (Optional) Zuweisen von Scalability-Servern zu virtuellen Desktops (siehe Seite 305).

Wichtig! Wenn Sie ein Golden Template unter Windows XP ausführen, starten Sie den Computer nach der DSM-Agent-Installation neu, um die "Tag Template"-Aktivierungsprozedur auszuführen.

Installieren des CA DSM-Agent VDI-Support-Add-on-Pakets

Installieren Sie das CA DSM-Agent VDI-Support-Add-on-Paket im Golden Template, um Software-Neuinstallation und Integration zwischen CA ITCM und VMware View oder Citrix XenDesktop zu ermöglichen. Der Add-On ermöglicht dem DSM-Agenten, die virtuelle Desktop-Umgebung zu verwenden und zu verwalten.

Das CA DSM-Agent VDI-Support-Add-on-Paket führt die folgenden Tasks aus:

- Aktiviert die Verwendung der Softwarestatus-Datenbank und richtet bei Bedarf die Pfade ein.
- Legt den Agenten auf den Golden Template-Modus fest.
- Kopiert ein Set von Klonskripten zum Golden Template, die während der Software-Neuinstallation verwendet werden.

Gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste in DSM-Explorer auf das Golden Template, und wählen Sie "Software-Jobs", "Softwarepaket bereitstellen" aus.

   Der Assistent zum Bereitstellen von Softwarepaketen wird geöffnet.

2. Befolgen Sie die Anleitungen des Assistenten. Geben Sie die folgenden Tasks im Assistenten an:

   - Wählen Sie das CA DSM-Agent VDI Support-Add-on Windows ENU-Paket unter "DSM-Softwarepakete" aus.

     Hinweis: Das Paket bietet eine allgemeine Lösung für VMware View und für Citrix XenDesktop und unterstützt außerdem Sysprep-Einstellungen auf VMware View.

   - Legen Sie den Zeitplan fest, und geben Sie den Jobcontainernamen ein.

3. Klicken Sie auf "Fertig stellen".

   Das Dialogfeld "Jobs einrichten" wird geöffnet.

4. Klicken Sie auf "OK".

   Das Paket wird zur geplanten Zeit zugestellt.

5. Wählen Sie das Golden Template, "Jobs", "Software-Jobs" in DSM-Explorer aus, um den Jobstatus zu überwachen.

Bereitstellen von Produktions-Softwarepaketen im Golden Template

Sie können Software Delivery verwenden, um Produktionssoftwarepakete im Golden Template bereitzustellen. Die Software-Anwendungen, die im Golden Template installiert werden, sind automatisch auf den virtuellen Desktops verfügbar, die aus dem Golden Template erstellt werden.

Gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste in DSM-Explorer auf das Golden Template, und wählen Sie "Software-Jobs", "Softwarepaket bereitstellen" aus.

   Der Assistent zum Bereitstellen von Softwarepaketen wird geöffnet.

2. Befolgen Sie die Anleitungen des Assistenten. Geben Sie die folgenden Aktionen im Assistenten an:

   - Wählen Sie die Softwarepakete und Prozeduren aus, die bereitgestellt werden sollen.
   - Geben Sie einen Name für den Jobcontainer ein.

3. Öffnen Sie das Dialogfeld mit den erweiterten Jobeinstellungen, und klicken Sie auf "Fertig stellen".

   Das Dialogfeld "Jobs einrichten" wird geöffnet.

4. Klicken Sie auf die "Jobs", "Joboptionen", Option "Pakete in der Staging-Bibliothek des Scalability-Servers speichern".

5. Klicken Sie auf "OK".

   Die angegebenen Pakete werden auf dem Scalability-Server des Golden Templates durch Staging bereitgestellt. Das Paket wird zur geplanten Zeit zugestellt.

Konfigurieren der Software-Neuinstallation

Software, die auf nicht persistenten virtuellen Desktops installiert wird, geht nach dem Neustart oder Abmelden oder nach einer Desktop-Aktualisierung mit einer neueren Version des Golden Templates verloren. Sie können CA ITCM konfigurieren, um die Software in solchen Fällen erneut zu installieren. CA ITCM verwendet eine Instanz-Softwarestatusdatenbank, die die Informationen aller Software-Jobs, die der Agent auf den virtuellen Desktops ausführt, enthält. Die virtuellen Desktops schließen die Details von der Instanz-Softwarestatusdatenbank und den Ausführungskontext ein. Diese Information ist wichtig für CA ITCM, um die Software erneut zu installieren.

Je nach Desktop-Virtualisierungslösung und den Desktop-Pool/Gruppeneinstellungen konfigurieren Sie die Software-Neuinstallation auf unterschiedliche Weise:

VMware View

- Führen Sie für Desktop-Gruppen mit *Quickprep*-Benutzeranpassung eine der folgenden Konfigurationsaufgaben aus:
  - Konfigurieren der Parameter für die Software-Neuinstallation in der Konfigurationsrichtlinie (siehe Seite 299)
  - Konfigurieren der Pooleinstellungen zum Ausführen von Compose.bat auf den virtuellen Desktops (siehe Seite 297)

  Hinweis: Wenn Sie sowohl die Richtlinie als auch die Pooleinstellungen konfigurieren, haben die Pooleinstellungen Vorrang.
- Führen Sie für Desktop-Gruppen mit *sysprep*-Benutzeranpassung die folgende Konfigurationsaufgabe aus:
  - Konfigurieren der Parameter für die Software-Neuinstallation in der Konfigurationsrichtlinie (siehe Seite 299)

Citrix XenDesktop

- Führen Sie für von MCS erstellte Desktops die folgende Konfigurationsaufgabe aus:
  - Konfigurieren der Parameter für die Software-Neuinstallation in der Konfigurationsrichtlinie (siehe Seite 299)
- Führen Sie für vDisk-basierte Desktops eine der folgenden Konfigurationsaufgaben aus:
  - Konfigurieren der Parameter für die Software-Neuinstallation in der Konfigurationsrichtlinie (siehe Seite 299)
  - Konfigurieren der Persönlichkeitsdaten auf den Zielgeräten (siehe Seite 302)

  Hinweis: Wenn Sie sowohl die Richtlinie als auch die Persönlichkeitsdaten konfigurieren, haben die Persönlichkeitsdaten Vorrang.

Hinweis: Sie können auch andere Konfigurationsrichtlinien ändern. Weitere Informationen zu diesen Richtlinien finden Sie unter Konfigurationsrichtlinien für die Unterstützung der Desktop-Virtualisierung (siehe Seite 308).

Konfigurieren der Pooleinstellungen zum Ausführen von Compose.bat auf den virtuellen Desktops

Geben Sie den folgenden Befehl im Post-Synchronisierungsskript unter "Guest Customizations" (Gast-Benutzeranpassungen) an, wenn Sie den Pool erstellen:
`Compose.bat [ISDBPath=<Path>] [Run=<Run>] [ISDBUser=<User> ISDBPassword=<Password>]`

ISDBPATH

Gibt den Pfad an, wo die Instanz-Softwaredatenbank gespeichert ist. Der Pfad kann lokal oder im Netzwerk sein, je nach Pooltyp. Geben Sie einen Netzwerkpfad für nicht persistente Pools und lokale oder Netzwerkpfade für persistente Pools an. Umgebungsvariablen und vordefinierte Makros wie {SCALABILITY_SERVER} und {POOL_NAME} sind als Teil des Pfads zulässig.

Beispiel: \\{SCALABILITY_SERVER}\%COMPUTERNAME%

Wichtig! Wenn unter Windows 7 der Pfadparameter die %USERNAME%-Umgebungsvariable enthält, geben Sie diesen Parameter nicht als Befehlszeilenparameter an Compose.bat weiter. Schließen Sie stattdessen alle Parameter in die Compose.bat-Datei ein (nur für VMware View).

{SCALABILITY_SERVER}

Gibt den Scalability-Server zurück, dem der virtuelle Desktop berichtet. Standardmäßig erteilen virtuelle Desktops dem gleichen Scalability-Server eine Meldung, dem das Golden Template eine Meldung erteilt. Wenn Sie die Scalability-Server-Zuweisung ausdrücklich geändert (siehe Seite 305) haben, gibt das Makro den Namen des neuen Scalability-Servers zurück.

{POOL_NAME}

Gibt den Poolnamen des virtuellen Desktop zurück. Dieses Makro ist nur für VMware View anwendbar.

Persistente Verwendung

Umgebungsvariablen, wie %COMPUTERNAME%, können als Bestandteil des ISDB-Pfads verwendet werden.

Beispiel: \\MachineName\{POOL_NAME}\%COMPUTERNAME%

Diese Option hat einen für einen Benutzer (da ein persistenter virtueller Desktop im demselben Benutzer zugewiesen ist) eindeutigen Pfad zur Folge.

Nicht persistente Verwendung

Die benutzerspezifischen Umgebungsvariablen, %USERNAME% und %USERDOMAIN%, können einbezogen werden, um die Softwarestatus-Datenbank für einen bestimmten Benutzer eindeutig zu identifizieren.

Beispiel: \\MachineName\{POOL_NAME}\%USERNAME%

Hinweis: Gehen Sie bei der Auswahl des Speicherorts im Falle von Netzwerkfreigabepfaden mit Bedacht vor, wenn einem einzelnen Benutzer mehrere Desktop-Pools zugewiesen sind. Sie müssen sicherstellen, dass der Softwarestatus des durch einen Benutzer in einem Pool verwendeten virtuellen Desktops nicht durch die Daten eines anderen virtuellen Desktops überschrieben wird, der durch denselben Benutzer in einem anderen Pool verwendet wird. Angenommen, "User1" ist befugt für die nicht persistenten Pools "poolA" und "poolB". Wenn der Pfad für beide Pools als "//<computer-name>/<freigabe-name>/Database/%USERNAME%" angegeben ist, kann der Softwarestatus von "User1" überschrieben werden, wenn sich der Benutzer anmeldet und beide virtuellen Desktops und beide Pools verwendet. Stellen Sie daher sicher, dass Sie wie folgt unterschiedliche Pfade definieren:

- "/<computer-mname>/<freigabe-name>/PoolA/%USERNAME%"
- "/<computer-mname>/<freigabe-name>/PoolB/%USERNAME%"

ISDBUSER

Gibt den Benutzernamen an, um eine Verbindung mit dem Instanz-Softwaredatenbankpfad in einer Netzwerkfreigabe aufzunehmen. Der Benutzername muss mithilfe des Befehls "sd_acmd encrypt" verschlüsselt werden.

ISDBPASSWORD

Gibt das Kennwort an, um eine Verbindung mit dem Instanz-Softwaredatenbankpfad in einer Netzwerkfreigabe aufzunehmen. Das Kennwort muss mithilfe des Befehls "sd_acmd encrypt" verschlüsselt werden.

RUN

Gibt an, wann der Offline-RAC-Prozess (Neuinstallation nach Absturz) ausgeführt werden soll. Gültige Werte sind "OnRecompose" und "OnLogon".

OnRecompose

Gibt an, dass der Offline-RAC initiiert wird, wenn der Desktop nach einer Aktualisierung oder Neuzusammenstellung gestartet wird. Verwenden Sie diese Option für Desktop-Gruppen, bei denen die Desktop-Zuweisung zu Benutzern festgelegt ist, beispielsweise bei persistenten verknüpften Klonen.

OnLogon

Gibt an, dass die Neuinstallation nach Absturz bei der Benutzeranmeldung ausgeführt wird.

Verwenden Sie diese Option für Desktop-Gruppen, bei denen sich die Desktop-Zuweisung zu Benutzern von Sitzung zu Sitzung unterscheidet, beispielsweise bei nicht persistenten Desktops.

Beispiele:

- **Persistente Verwendung:** Compose.bat "ISDBPath=<Path>" "Run=OnRecompose"
- **Nicht persistente Verwendung:** Compose.bat "ISDBPath=<Path>" "Run=OnLogon"

Konfigurieren der Parameter für die Software-Neuinstallation in der Konfigurationsrichtlinie

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM", "Software Delivery", "Agent".
2. Wählen Sie die Einstellungen für RAC: Software-Neuinstallation für virtuelle Rechner aus, um die folgenden Attribute anzuzeigen:

   Agenten-Namensgebungsmuster

   Gibt das Agenten-Namensgebungsmuster des virtuellen Desktops an. Für VMware View muss das Namensgebungsmuster *name-{n}* sein und für XenDesktop muss das Namensgebungsmuster *name##* sein. Sie können diesen Platzhalter (#) nicht am Anfang oder mehr als einmal angeben.

   Von:

   Gibt den Startbereich an, dessen Desktops eingeschlossen werden. Der Bereich kann eine Zahl sein; XenDesktop lässt Sie auch ein Alphabet angeben. *Von* gibt den Anfang des Namensgebungsmusters an. Der Anfang und die Platzhalterlänge müssen gleich sein, *Bis* kann größer sein als die Platzhalterlänge.

   Bis

   Gibt den Endbereich an, dessen Desktops eingeschlossen werden. Der Bereich kann eine Zahl sein; XenDesktop lässt Sie auch ein Alphabet angeben.

Beispiele: Agenten-Namensgebungsmuster für VMware View

Agenten-Namensgebungsmuster	Von:	Bis	Mögliche Desktop-Namen
Name-{n}	1	100	Name-1, Name-2….Name-100

Beispiele: Agenten-Namensgebungsmuster für Citrix XenDesktop

Agenten-Namensgebungsmuster	Von:	Bis	Mögliche Desktop-Namen
Name#	1	100	Name1, Name2, …..Name100
Name###	1	100	Name001, Name002…..Name100
Name##	AA	AZ	NameAC, NameAE,…NameAZ

Instanz-Softwaredatenbankpfad

Gibt den Pfad an, wo die Instanz-Softwaredatenbank gespeichert ist. Der Pfad kann lokal oder im Netzwerk sein, je nach Pooltyp. Geben Sie einen Netzwerkpfad für nicht persistente Pools und einen lokalen oder Netzwerkpfad für persistente Pools an (persistent verknüpfte Klone für VMware View und Differenzmodus-vDisk-basierte virtuelle Desktop-Gruppen für Citrix XenDesktop mit festgelegter Desktop-Zuweisung). In letzterem Fall ist die Angabe eines lokalen Pfades nur möglich, wenn die persistente, dem virtuellen Desktop zugeordnete Festplatte verfügbar ist. Umgebungsvariablen und vordefinierte Makros wie {SCALABILITY_SERVER}, {GROUP_NAME} und {POOL_NAME} sind als Teil des Pfades erlaubt.

Beispiel: \\{SCALABILITY_SERVER}\{GROUP_NAME}\%COMPUTERNAME%

{GROUP_NAME}

Gibt den Desktop-Gruppennamen des virtuellen Desktop zurück. Dieses Makro ist nur für Citrix XenDesktop anwendbar.

{POOL_NAME}

Gibt den Poolnamen des virtuellen Desktop zurück. Dieses Makro ist nur für VMware View anwendbar.

{SCALABILITY_SERVER}

Gibt den Scalability-Server zurück, dem der virtuelle Desktop berichtet. Standardmäßig berichten virtuelle Desktops dem gleichen Scalability-Server, dem das Golden Template oder vDisk berichtet. Wenn Sie die Scalability-Server-Zuweisung ausdrücklich geändert (siehe Seite 305) haben, gibt das Makro den Namen des neuen Scalability-Servers zurück.

Hinweis: Für XenDesktop können Sie einem einzelnen Desktop mehrere Benutzer in einer zusammengefassten statischen Gruppe zuweisen. Um in diesem Fall die Neuinstallation von benutzerinstallierter Software zu unterstützen, geben Sie den Instanz-Softwaredatenbankpfad in der folgenden Weise an: *<server_name>**%computername%**%username%.* Legen Sie außerdem den Ausführungskontext auf *OnLogon* fest.

Anwendername

Gibt den Benutzernamen an, um eine Verbindung mit dem Instanz-Softwaredatenbankpfad in einer Netzwerkfreigabe aufzunehmen. Der Benutzername wird mithilfe des Befehls "sd_acmd encrypt" verschlüsselt.

Kennwort

Gibt das Kennwort an, um eine Verbindung mit dem Instanz-Softwaredatenbankpfad in einer Netzwerkfreigabe aufzunehmen. Das Kennwort wird mithilfe des Befehls "sd_acmd encrypt" verschlüsselt.

Ausführen

Gibt an, wann der Offline-RAC-Prozess (Neuinstallation nach Absturz) ausgeführt werden soll. Erlaubte Werte sind "OnRecompose" und "OnLogon".

OnRecompose

Gibt an, dass die Neuinstallation nach Absturz gestartet wird, wenn der Desktop nach einer Aktualisierung oder Neuzusammenstellung (VMware View), Zurücksetzen des Desktops oder Snapshot-Aktualisierung (Citrix MCS) und Zurücksetzen des Desktops oder vDisk-Aktualisierung (gestreamte virtuelle Desktops) neu startet.

Verwenden Sie diese Option für Desktop-Gruppen, wo die Desktop-Zuweisung zu Benutzern festgelegt ist, wie persistente verknüpfte Klone, zusammengefasste statische Desktops und Desktops, die auf Differenzmodus-vDisks basieren.

OnLogon

Gibt an, dass die Neuinstallation nach Absturz bei der Benutzeranmeldung ausgeführt wird.

Verwenden Sie diese Option nur für zusammengefasste Desktop-Gruppen, wo die Desktop-Zuweisung zu den Benutzern sich von Sitzung zu Sitzung unterscheidet, wie nicht persistente Desktops, nach dem Zufallsprinzip zusammengefasste Desktops sowie zusammengefasste Desktops, die auf Standardmodus-vDisks basieren.

3. Speichern und versiegeln Sie die Richtlinie.

   Die Software-Neuinstallationskonfiguration wird auf das Golden Template angewandt.

Konfigurieren der Persönlichkeitsdaten auf den Zielgeräten

Konfigurieren Sie für Citrix XenDesktop die Persönlichkeitsdaten, sobald Sie die Kataloge mithilfe des XenDesktop-Setup-Assistenten oder des gestreamten VM-Setup-Assistenten erstellen und bevor die Desktop-Gruppen aus den Rechnern erstellt werden.

Gehen Sie wie folgt vor:

1. Öffnen Sie das Dialogfeld "Target Device Properties" in Citrix Provisioning Services Console für einen virtuellen Desktop.
2. Klicken Sie auf die Registerkarte "Personality", und fügen Sie die folgenden Parameter hinzu:

   CA_DSM_ISDBPATH

   Gibt den Pfad an, wo die Instanz-Softwaredatenbank gespeichert ist. Der Pfad kann lokal oder im Netzwerk sein, je nach Pooltyp. Geben Sie einen Netzwerkpfad für nicht persistente Pools und einen lokalen oder Netzwerkpfad für persistente Pools an (Differenzmodus-vDisk-basierte virtuelle Desktop-Gruppen für Citrix XenDesktop mit festgelegter Desktop-Zuweisung).

   In letzterem Fall ist die Angabe eines lokalen Pfades nur möglich, wenn die persistente, dem virtuellen Desktop zugeordnete Festplatte verfügbar ist. Umgebungsvariablen und vordefinierte Makros wie {{SCALABILITY_SERVER} und {GROUP_NAME} sind als Teil des Pfads zulässig.

   Beispiel: \\{SCALABILITY_SERVER}\{GROUP_NAME}\%COMPUTERNAME%

   {GROUP_NAME}

   Gibt den Desktop-Gruppennamen des virtuellen Desktop zurück. Dieses Makro ist nur für Citrix XenDesktop anwendbar.

   {SCALABILITY_SERVER}

   Gibt den Scalability-Server zurück, dem der virtuelle Desktop berichtet. Standardmäßig berichten virtuelle Desktops dem gleichen Scalability-Server, dem das Golden Template oder vDisk berichtet. Wenn Sie die Scalability-Server-Zuweisung ausdrücklich geändert (siehe Seite 305) haben, gibt das Makro den Namen des neuen Scalability-Servers zurück.

CA_DSM_ISDBUSER

Gibt den Namen des Instanz-Softwaredatenbankbenutzers in verschlüsselter Form an. Der Benutzername wird mithilfe des Befehls "sd_acmd encrypt" verschlüsselt.

CA_DSM_ISDBPASSWORD

Gibt das verschlüsselte Kennwort der Instanz-Softwaredatenbank in verschlüsselter Form an. Das Kennwort wird mithilfe des Befehls "sd_acmd encrypt" verschlüsselt.

CA_DSM_RUN

Gibt an, wann der Offline-RAC-Prozess (Neuinstallation nach Absturz) ausgeführt werden soll. Gültige Werte sind "OnRecompose" und "OnLogon".

OnRecompose

Gibt an, dass der Offline-RAC initiiert wird, wenn der Desktop nach einer Zurücksetzung oder Update (im Falle von Citrix MCS) des Snapshots bzw. nach einem vDisk-Update oder einer -Zurücksetzung (im Falle gestreamter virtueller Desktops) gestartet wird.

Verwenden Sie diese Option für Desktop-Gruppen, bei denen die Desktop-Zuweisung zu Benutzern festgelegt ist, wie zusammengefasste statische Desktops und Desktops, die auf Differenzmodus-vDisks basieren.

OnLogon

Gibt an, dass die Neuinstallation nach Absturz bei der Benutzeranmeldung ausgeführt wird.

Verwenden Sie diese Option nur für zusammengefasste Desktop-Gruppen, bei denen die Desktop-Zuweisung zu den Benutzern sich von Sitzung zu Sitzung unterscheidet, beispielsweise bei nach dem Zufallsprinzip zusammengefasste Desktops sowie zusammengefasste Desktops, die auf Standardmodus-vDisks basieren.

3. Speichern Sie die Eigenschaften.

   Der virtuelle Desktop wird konfiguriert, um die Details der Instanz-Softwarestatusdatenbank einzuschließen.

4. Führen Sie eine der folgenden Aufgaben aus:

   - Führen Sie Schritte 1 bis 3 auf allen virtuellen Desktops aus.
   - Kopieren Sie die Parameter von einem Desktop auf alle virtuellen Desktops.

Sie haben jetzt Persönlichkeitsdaten auf den Zielgeräten konfiguriert.

Streaming von Persönlichkeitsdaten zu virtuellen Desktops in XenDesktop 5.0 und 5.5

Mit Citrix XenDesktop Virtual Desktop Agent 5.0 und Virtual Desktop Agent 5.5 werden Persönlichkeitsdaten für virtuelle Desktops anfangs nicht zu den virtuellen Desktops gestreamt.

Wenn die Instanz-Softwaredatenbankkonfiguration mithilfe von Persönlichkeitsdaten erfolgt und nicht durch die Konfigurationsrichtlinie, ist die Software-Neuinstallationfunktionalität betroffen.

Verwenden Sie die folgenden Hotfixes des Citrix Virtual Desktop Agent, um dieses Problem zu beheben.

- http://support.citrix.com/article/CTX131268 (32-Bit-Version)
- http://support.citrix.com/article/CTX131269 (64-Bit-Version)

Unterstützte virtuelle Desktop-Typen für die Software-Neuinstallation

CA ITCM unterstützt Software-Neuinstallation auf den folgenden virtuellen Desktop-Typen:

VMware View:

- Verknüpfte Klone

Citrix XenDesktop:

- Zusammengefasste statische Desktops
- Zusammengefasste Desktops nach dem Zufallsprinzip
- Gestreamte Desktops
- Vorhandene katalogbasierte Desktops auf Standard- oder Differenzmodus-vDisk

Hinweis: Sie können die folgenden Typen aus dem Golden Template erstellen, aber es wird keine Unterstützung für die Software-Neuinstallation benötigt. Dem Domänen-Manager wird beim Starten nur über die Vorlagesoftwaredatensätze berichtet. Sie können die folgenden Typen unabhängig als normale CA ITCM-Agenten verwalten.

- Privatmodus-vDisk-Desktops
- Dedizierte Desktops (durch MCS)

Wichtig! Stellen Sie sicher, dass die virtuellen Desktops so konfiguriert sind, dass sie neu gestartet werden, wenn der Benutzer sich aufgrund unverankerter verknüpfter Klone in VMware View abmeldet. Wenn Sie zusammengefasste statische Gruppen mit einem mehreren Benutzern zugewiesenen Desktop erstellen, geben Sie diese Einstellung manuell an, damit die Software-Neuinstallation wie erwartet funktioniert.

(Optional) Zuweisen von Scalability-Servern zu virtuellen Desktops

Jeder virtuelle Desktop berichtet dem gleichen Scalability-Server wie der Agent des Golden Templates oder die vDisk. Sie können den Agenten auf dem virtuellen Desktops verschiedene Scalability-Server zuweisen, um die Last auf dem Server zu verteilen. Bevor Sie fortfahren können, müssen Sie das Namensgebungsmuster für Desktops festgelegt haben, die aus dem Golden Template erstellt werden. Basierend auf den Namensgebungsmustern des Desktops können Sie den Agenten auf dem Desktop verschiedene Scalability-Server zuweisen. Sie können auch die Anzahl von Desktops konfigurieren, die Sie dem Server zuweisen möchten.

Gehen Sie wie folgt vor:

1. Öffnen Sie in DSM-Explorer die Konfigurationsrichtlinie, die Sie auf das Golden Template anwenden möchten.
2. Navigieren Sie zu "DSM", "Allgemeine Komponenten", "Registrierung".
3. Doppelklicken Sie auf die Scalability-Server-Konfigurationsrichtlinie.
4. Klicken Sie auf "Zeile hinzufügen", und geben Sie das Namensgebungsmuster und den Bereich in den folgenden Feldern an:

   Agenten-Namensgebungsmuster

   Gibt das Agenten-Namensgebungsmuster des virtuellen Desktops an. Für VMware View muss das Namensgebungsmuster wie name-{n} sein und für XenDesktop muss das Namensgebungsmuster wie name## sein. Sie können sich auch für ein anderes Namensgebungsmuster entscheiden.

   Scalability-Server

   Gibt den Scalability-Server an, den Sie für das angegebene Muster und den Bereich zuweisen möchten.

   Von:

   Gibt den Startbereich an, dessen Desktops eingeschlossen werden. Der Bereich kann eine Zahl sein; Citrix XenDesktop lässt Sie auch ein Alphabet angeben. Der Anfang und die Platzhalterlänge müssen gleich sein, *Bis* kann größer sein als die Platzhalterlänge.

   Bis

   Gibt den Endbereich an, dessen Desktops eingeschlossen werden. Der Bereich kann eine Zahl sein; Citrix XenDesktop lässt Sie auch ein Alphabet angeben.

Beispiele: Agenten-Namensgebungsmuster für Citrix XenDesktop

Agenten-Namensgebungsmuster	Von:	Bis	Mögliche Desktop-Namen
Name#	1	100	Name1, Name2, Name100
Name###	1	100	Name001, Name002, Name100
Name##	AB	BC	NameAC, NameAE, NameAZ

Beispiele: Agenten-Namensgebungsmuster für VMware View

Agenten-Namensgebungsmuster	Von:	Bis	Mögliche Desktop-Namen
Name-{n}	1	100	Name-1, Name-2, Name-100

5. Speichern und versiegeln Sie die Richtlinie.

   Wenn virtuelle Desktops erstellt werden, werden sie automatisch einem Scalability-Server zugewiesen, je nach angegebener Konfiguration.

Konfigurieren der Inventarerfassung bei Software-Neuinstallation

Konfigurieren Sie die Inventarerfassung, um das Inventar vom virtuellen Desktop zu erfassen, entweder sofort nach der Neuinstallation nach Absturz (RAC) oder wenn der Benutzer sich nach RAC anmeldet. Inventarerfassung hilft Ihnen zu überprüfen, ob alle Software-Anwendungen neu installiert wurden.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM", "Software Delivery", "Agent".
2. Wählen Sie die Konfigurationsrichtlinie für RAC: Inventarerfassung nach Neuinstallation aus, und legen Sie den Wert auf eines der folgenden Attribute fest:

   Nein

   Gibt an, dass das Inventar nicht nach Neuinstallation erfasst wird, sondern während der normalen Ausführung des AM-Agenten, der nach RAC oder vor RAC ausgeführt werden kann.

   Sofort

   Gibt an, dass das Inventar nach der Software-Neuinstallation sofort erfasst wird. Berichtet über die neu installierte Software als Teil von Softwareinventar- und Client-Geräteinformationen wie IP, MAC-Adress, und Hostname erst nach der Benutzeranmeldung.

   Nach Benutzeranmeldung

   Gibt an, dass das Inventar nur erfasst wird, wenn der Benutzer sich nach RAC anmeldet. Über die neu installierte Software und Client-Geräteinformationen wird berichtet, nachdem der Benutzer sich angemeldet hat.

   Die Inventarerfassung nach RAC erfolgt basierend auf der von Ihnen angegebenen Konfiguration.

Kennzeichnen der Vorlage und Erstellen eines Snapshots oder vDisks

Durch Kennzeichnen mit einem Tag können Sie die Version der Vorlage verfolgen, die von den virtuellen Desktops verwendet wird. Kennzeichnen Sie die Vorlage, um einen Vorlagetag zu generieren, und ordnen Sie die virtuellen Desktops ihrem übergeordneten Golden Template zu.

Gehen Sie wie folgt vor:

1. Ziehen Sie den Vorgang für die Tag-Vorlage vom CA DSM-Agent-Add-On-VDI-Paket zum Golden Template im DSM-Explorer.

   Der Vorgangsstatus wird angezeigt, nachdem der Vorgang ausgeführt wurde.

2. Führen Sie eine der folgenden Aktionen aus, je nach Desktop-Virtualisierungslösung:

   - (Für XenDesktop mithilfe von Citrix Provisioning Services) Erstellen Sie die vDisk mithilfe von XenConvert oder einem anderen geeigneten Imaging-Tool.
   - (Für VMware View und Citrix MCS) Fahren Sie den virtuellen Rechner herunter, und erstellen Sie einen Snapshot.

   Diese Aktion ordnet den Snapshot oder die vDisk dem Vorlage-Tag zu.

Der Snapshot oder die vDisk wird erstellt und dem Golden Template anhand des Vorlage-Tags zugeordnet.

Wichtig!

- Wenn Sie ein Golden Template unter Windows XP ausführen, starten Sie den Computer nach der DSM-Agent-Installation neu, um die "Tag Template"-Aktivierungsprozedur erfolgreich auszuführen.
- Für VMware View müssen nicht persistente Desktop-Pools mit der Option "Power off and delete virtual machine after first use" (Virtuelle Computer nach erster Verwendung ausschalten und löschen) in VMware View 4.0 erstellt werden. Andernfalls funktioniert die Offline-RAC-Funktion nicht. Wählen Sie in VMware View 4.5 stattdessen die Option "Delete or refresh desktop on logoff" (Desktop bei Abmeldung löschen oder aktualisieren), und legen Sie sie entweder auf "Refresh Immediately" (Sofort aktualisieren) oder "Delete Immediately" (Sofort löschen) fest.

Überprüfen der Golden Template-Zuweisung

Sie können das zugewiesene Golden Template unter "Inventar", "Vorlageneinstellungen" überprüfen.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Computer und Benutzer", "Alle Computer", "*Computername*", "Inventar".
2. Klicken Sie auf die Registerkarte "System", "Vorlageneinstellungen".

   Die Liste der zugewiesenen Vorlagen wird angezeigt.

Das Golden Template wird jetzt für das Verwalten der virtuellen Desktops vorbereitet.

Konfigurationsrichtlinien für die Unterstützung der Desktop-Virtualisierung

Nachdem Sie das CA DSM-Agent VDI-Support-Add-on-Paket installiert haben, konfigurieren Sie CA ITCM-Konfigurationsrichtlinien für virtuelle Desktops. Einige dieser Richtlinien sind obligatorisch und von VMware View voreingestellt. Andere Richtlinien sind optional und erfordern Eingaben laut Dokumentation.

Eine neue Registrierungsrichtliniengruppe wurde hinzugefügt und andere Konfigurationsrichtliniengruppen wurden erweitert, um die Verwaltung von virtuellen Desktops zu unterstützen, die von Citrix XenDesktop und VMware View bereitgestellt werden.

Hinweis: Wenden Sie die Konfigurationsrichtlinien auf die Agenten der geklonten virtuellen Desktops und auf die Agenten der Golden Templates an. Dieser Prozess muss vor dem Speichern des Golden Template-Snapshots erfolgen, mit Ausnahme der obligatorischen lokal verwalteten Richtlinien, die von den Klonskripten voreingestellt werden.

Die Richtlinie wird nicht automatisch von den geklonten virtuellen Desktops aus dem Golden Template übernommen. Wenn die Werte der geklonten virtuellen Desktop und der zentral verwalteten Richtlinien unterschiedlich sind, werden die Werte bald nach der Registrierung beim Manager überschrieben.

Registrierungs-Richtliniengruppe

Eine neue Richtlinienuntergruppe "Registrierung" ist unter der Richtliniengruppe "Allgemeine Komponenten" für virtuelle Desktop-spezifische Identifizierung hinzugefügt worden. Die Richtliniengruppe "Registrierung" enthält die folgenden Richtlinien:

Hostschlüssel

Definiert eine Zeichenfolge, die verwendet wird, um einen geklonten Rechner eindeutig zu identifizieren. Ein Hostschlüssel ist für verknüpfte Klone erforderlich, weil bei jeder Neuzusammenstellung des virtuellen Desktops ein neuer virtueller Rechner generiert wird, der einen neuen eindeutigen Computer in der MDB registriert. Das Ergebnis ist, dass der Domänen-Manager im Laufe der Zeit viele Computer sehen würde, die nicht mehr vorhanden sind. Wenn der Hostschlüssel verwendet wird, werden die vorhandenen Computerdatensätze für die virtuellen Desktops in der MDB im Laufe der Zeit wieder benutzt.

Ein Hostschlüssel enthält einfachen Text plus eine Anzahl von Makros. Bei der Registrierung blendet CAF die Makros ein und sendet das Ergebnis an den Scalability-Server. Die Engine verwendet dann den Hostschlüssel statt Host-UUID/Hostnamen/MAC-Adresse, um Assets in der MDB zu identifizieren. Von jetzt an identifiziert der Hostschlüssel den Agenten.

Hinweis: In typischen Szenarien wird die MAC-Adresse während der Neuzusammenstellung von persistent verknüpften Klonen nicht geändert. Allerdings ändert VMware in einigen Fällen die MAC-Adresse der persistent verknüpften Klone während der Neuzusammenstellung. Deswegen ist die Verwendung eines Hostschlüssels normalerweise sowohl für nicht persistente als auch für persistent verknüpfte Klone und für MCS-basierte virtuelle Desktops nötig.

Verwenden Sie die folgenden Makros:

Umgebungsvariable: $env(name)

Beispiel: $env("COMPUTERNAME")-VDI

Registrierungsschlüssel: $reg(key,value)

Beispiel: $reg("HKLM\SOFTWARE\CA\GuestID," GuestUUID")-VDI

INI-Dateiwert: $ini(path,section,key)

Beispiel: $ini("c:\id.ini","identity","uuid")-VDI

Diese Makros können auch in einer Zeichenfolge kombiniert werden.

Beispiel: $env("COMPUTERNAME")-
$reg("HKLM\SOFTWARE\CA\GuestID","GuestUUID")-VDI

Hinweis: Standardmäßig legt das CAFPostInit.dms-Skript den Hostschlüssel auf dem Agenten mit $env("COMPUTERNAME") fest. Daher müssen Sie diese Richtlinie nicht ändern. Wenn Sie jedoch ein anderes Makro verwenden möchten, überprüfen Sie, dass alle generierten Hostschlüssel durch die Verwendung der entsprechenden Host-Makrozeichenfolgen im CAFPostInit.dms-Skript eindeutig sind. Überprüfen Sie auch, dass der Hostschlüssel nicht länger als 64 Zeichen ist.

Standard: leer, <Lokal verwaltet>

Scalability-Server-Konfiguration

Erlaubt dem Administrator, den Agent-Scalability-Server zu konfigurieren, der auf dem virtuellen Rechner-Namensgebungsmuster basiert, das für den Desktop-Pool und -Bereich verwendet wird. Sie können mehrere Bereiche anwenden. Diese Richtlinie ist optional, und wenn kein Wert festgelegt wird, berichten alle Klone dem gleichen Scalability-Server wie der Agent des Golden Templates, aus dem sie geklont worden sind. Weitere Informationen finden Sie unter Scalability-Server-Konfiguration.

Richtliniengruppe "Software Delivery (Agent)"

Die Richtliniengruppe "Software Delivery (Agent)" wurde erweitert, um die folgenden Konfigurationsrichtlinien für das Verwalten des Software Delivery-Agenten in VMware View-Umgebungen einzuschließen.

Hinweis: Die RAC-Konfigurationsrichtlinien in der Richtliniengruppe "Agent" gelten nur für die Neuinstallation nach Absturz (Offline-RAC). Die herkömmliche RAC-Funktionalität wird von den Richtlinien in der Richtliniengruppe "Software Delivery (Manager)" konfiguriert.

Sie können Richtlinienparameterwerte ändern, indem Sie auf eine Richtlinie doppelklicken, um das Dialogfeld "Eigenschaften von Einstellung" anzuzeigen.

RAC: Verhalten für mehrere Einträge der gleichen Aktivierungs-/Konfigurationsprozedur

Gibt an, ob doppelte Softwareprozeduren während Offline-RAC ausgeschlossen werden.

In Software Delivery darf eine Installationsprozedur nur einmal ausgeführt werden, aber Aktivierungs- und Konfigurationsprozeduren können mehrmals ausgeführt werden. Wenn der Agent den RAC-Container für ein Softwarepaket vorbereitet, können mehrere Aktivierungs- und Konfigurationsprozeduren eingeschlossen werden. Der Wert, der für diese Richtlinie festgelegt ist, bestimmt, wie doppelte Aktivierungs-/Konfigurationsprozeduren innerhalb eines einzelnen Softwarepakets gehandhabt werden. Folgende Werte sind gültig:

Jeden duplizierten Aktivierungs-/Konfigurationsvorgang neu ausführen

Gibt an, dass alle in der Datenbank aufgezeichneten Aktivierungs-/Konfigurationsprozeduren ausgeführt werden.

Nur den ersten duplizierten Aktivierungs-/Konfigurationsvorgang neu ausführen

Gibt an, wenn Aktivierungs-/Konfigurationsprozeduren mehr als einmal vorhanden sind, wird nur das erste Duplikat ausgeführt.

Nur den letzten duplizierten Aktivierungs-/Konfigurationsvorgang neu ausführen

Gibt an, wenn Aktivierungs-/Konfigurationsprozeduren mehr als einmal vorhanden sind, wird nur das letzte Duplikat ausgeführt.

Standard: Jeden duplizierten Aktivierungs-/Konfigurationsvorgang neu ausführen

RAC: Container-Typ

Gibt an, ob der Agent Software-Jobs im Offline-RAC-Container als ein Batch oder ohne Verknüpfung ausführt. Folgende Werte sind gültig:

Batch

Gibt an, dass alle Jobs nacheinander als eine Arbeitseinheit für jedes Ziel ausgeführt werden. Wenn ein Job in der Sequenz fehlschlägt, dann werden die verbleibenden Jobs für dieses Ziel nicht ausgeführt.

Keine Verknüpfung

Gibt an, dass die Jobs nacheinander, aber unabhängig voneinander ausgeführt werden.

Standard: Batch

RAC: Software-Prozedur im Falle eines Fehlers aus Softwarestatusdatenbank löschen

Steuert, ob die Softwarestatusdatenbank aktualisiert wird, wenn ein oder mehrere Jobs im RAC-Container fehlschlagen. Wenn "True" (Wahr) festgelegt ist, werden die fehlgeschlagenen Jobeinträge aus der Softwarestatusdatenbank gelöscht. Bei "False" (Falsch) bleiben die fehlgeschlagenen Einträge.

Standard: True

RAC: Jobprüfungs-GUI beibehalten, bis Endbenutzer schließt

Steuert, ob das Dialogfeld "Software Delivery - Jobprüfung" wartet, bis der Benutzer das Dialogfeld schließt, falls RAC während einer Neuinstallation im interaktiven Modus fehlschlägt. Zum Beispiel stellt der Wert "True" (Wahr) sicher, dass ein RAC-Fehler nicht übersehen wird, wenn der Benutzer nicht am Computer ist.

Standard: True

RAC: Verwalten der Vorinstallations-Softwarestatusdatenbank

Definiert, ob eine Vorinstallations-Softwarestatusdatenbank beibehalten wird, wenn den virtuellen Desktops keine Benutzer zugewiesen sind. Eine Vorinstallations-Softwarestatusdatenbank ist nützlich, wenn virtuelle Desktops in einem Pool erstellt werden und als Agenten registriert werden, aber noch nicht Benutzern zugewiesen sind. Eine Vorinstallations-Datenbank ist nützlich für den Administrator, um erforderliche Softwarepakete zu den virtuellen Desktops zu übertragen.

Bei der Einstellung "True" (Wahr) wird eine Vorinstallations-Softwarestatusdatenbank auf dem lokalen Dateisystem beibehalten, bevor ein Benutzer dem virtuellen Desktop zugewiesen wird. Die Vorinstallations-Datenbank wird mit der zugewiesenen Benutzerinstanz-Softwarestatusdatenbank zusammengeführt, wenn der Benutzer sich zum ersten Mal anmeldet.

Wenn "False" (Falsch) festgelegt ist, gelten die folgenden Bedingungen.

Persistente Desktops:

Für persistente Desktops gilt, wenn Offline-RAC für die Ausführung bei Anmeldung konfiguriert ist, werden diese Softwarepakete neu installiert, wenn diese Richtlinie auf "False" (Falsch) festgelegt ist, weil die Software-Job-Datensätze zur Instanzdatenbank statt zur Vorinstallations-Datenbank hinzugefügt werden.

Nicht persistente Desktops:

Für nicht persistente Desktops gilt, wenn diese Richtlinie auf "False" (Falsch) festgelegt ist, werden Software Delivery-Jobdatensätze für diese Softwarepakete nicht beibehalten. Überdies können sie nicht neu installiert werden, wenn der virtuelle Desktop später aktualisiert wird.

Standard: True

RAC: Softwarestatusdatenbank beibehalten

Steuert, ob der Software Delivery-Agent eine Datenbank seines Status beibehält, ungeachtet der VMware View-Funktionalität.

Hinweis: Diese Richtlinie ist obligatorisch und von den VMware View-Integrationsskripten auf "True" (Wahr) eingestellt. Ändern Sie den eingestellten Wert nicht manuell.

Standard: Falsch, <Lokal verwaltet>

RAC: Maximale Wiederholungsdauer in Sekunden

Gibt die maximale Zeitspanne in Sekunden zwischen den Versuchen eines Agenten an, sich während einer Jobprüfung mit dem Scalability-Server in Verbindung zu setzen. Diese Richtlinie funktioniert mit der Richtlinie für RAC: Anzahl der Wiederholungsversuche für die Neuinstallation nach Absturz (Offline-RAC). Die Wiederherstellung der Verbindung wird versucht, bis das von einer dieser Richtlinien angegebene Limit erreicht ist.

Standard: 60

RAC: Anzahl von Wiederholungen im Fall von Offline-RAC

Definiert die Höchstanzahl von Verbindungswiederholungen, die ein Agent während einer Jobprüfung am Scalability-Server versuchen kann. Diese Richtlinie funktioniert mit der Richtlinie für RAC: Maximale Wiederholungsdauer in Sekunden. Die Wiederherstellung der Verbindung wird versucht, bis das von einer dieser Richtlinien angegebene Limit erreicht ist.

Standard: 100

RAC: Kennwort zum Zugriff auf die Instanz-Softwarestatusdatenbank

Gibt das Kennwort des Benutzers mit Zugriffsberechtigungen für die Instanz-Softwarestatusdatenbank an. Die Kennwortzeichenfolge wird verschlüsselt. Wenn angegeben, verwendet der Agent diese Anmeldeinformationen, um auf die Netzwerkfreigabe zuzugreifen.

Wir empfehlen, dass Sie das Kennwort zuerst mit dem Befehl "sd_acmd encrypt" verschlüsseln. Geben Sie dann das verschlüsselte Kennwort als einer der Parameter an, wenn das Compose.bat-Skript ausgeführt wird, das wiederum den Konfigurationsparameter festlegt.

Wenn das Kennwort für den Speicherort der Freigabe das gleiche für alle aus einem bestimmten Golden Template-Snapshot erstellten Desktop-Pools ist, können Sie alternativ das Kennwort in der Konfigurationsrichtlinie festlegen. Wenden Sie dann die Richtlinie auf das Golden Template und die geklonten virtuellen Desktops an.

Standard: leer, <Lokal verwaltet>

RAC: Pfad zur Instanz-Softwarestatusdatenbank

Gibt den Installationspfad für die Instanz-Softwarestatusdatenbank an. Der angegebene Pfad kann eingebettete Umgebungsvariablen, zum Beispiel "\\Fileserver1\Share1\%COMPUTERNAME%\InstanceSoftwareDatabase" einschließen.

Hinweis: Diese Richtlinie ist obligatorisch, aber geben Sie den Pfad manuell als einen der Parameter ein, wenn das Compose.bat-Skript ausgeführt wird. Dieses Skript legt wiederum den Konfigurationsparameter fest.

Standard: leer, <Lokal verwaltet>

RAC: Pfad zur Vorlage-Softwarestatusdatenbank

Gibt den Installationspfad für die Vorlage-Softwarestatusdatenbank an. Wenn der Wert leer ist, verwendet der Agent den entsprechenden einheitenspezifischen Pfad, das heißt "<ITCM InstallDir>\SD\ASM\DATABASE\Agent\TemplateSoftwareDatabase".

Standard: leer, <Lokal verwaltet>

RAC: RAC-Richtlinieneinstellung des Agenten

Steuert die RAC-Richtlinieneinstellung des Software Delivery-Agenten. Bei der Einstellung "True" (Wahr) wird die RAC-Richtlinie des Agenten auf "Offline" gesetzt. Bei der Einstellung "False" (Falsch) wird die RAC-Richtlinie auf die Standard-RAC-Einstellung festgelegt.

Hinweis: Diese Richtlinie ist obligatorisch und von den VMware View-Integrationsskripten auf "True" (Wahr) eingestellt. Ändern Sie den eingestellten Wert nicht manuell.

Der hier festgelegte Wert entspricht standardmäßig der Registerkarte "Software Delivery" des Dialogfelds "Computereigenschaften".

Standard: Falsch, <Lokal verwaltet>

RAC: SD-Agent auf 'Golden Template'-Modus festlegen

Erlaubt dem Agenten, zwischen der Ausführung eines Golden Templates oder eines Klons zu unterscheiden. Bei "True" (Wahr) wird der Agent anhand eines Golden Templates ausgeführt.

Hinweis: Diese Richtlinie ist obligatorisch und wird von den VMware View-Integrationsskripten voreingestellt.

Standard: Falsch, <Lokal verwaltet>

RAC: Benutzername zum Zugriff auf die Instanz-Softwarestatusdatenbank

Gibt den Namen des Benutzers mit Zugriffsberechtigungen für die Instanz-Softwarestatusdatenbank an. Der Benutzername muss wie folgt formatiert werden: (*domainname* | local\)'user'. Die Zeichenfolge wird verschlüsselt. Wenn angegeben, verwendet der Agent diese Anmeldeinformationen, um auf die Netzwerkfreigabe zuzugreifen.

Wir empfehlen, dass Sie den Benutzernamen zuerst mit dem Befehl "sd_acmd encrypt" verschlüsseln. Geben Sie dann den verschlüsselten Benutzernamen als einer der Parameter an, wenn das Compose.bat-Skript ausgeführt wird, das wiederum den Konfigurationsparameter festlegt.

Wenn der Benutzername für den Speicherort der Freigabe der gleiche für alle aus einem bestimmten Golden Template-Snapshot erstellten Desktop-Pools ist, können Sie optional den Benutzernamen in der Konfigurationsrichtlinie festlegen. Wenden Sie dann die Richtlinie auf das Golden Template und die geklonten virtuellen Desktops an.

Hinweis: Standardmäßig schließen die Berechtigungen für einen freigegebenen Ordner nur die Gruppe "Alle" mit Lesezugriffs-Berechtigungen ein. Um sicherzustellen, dass die Instanz-Softwarestatusdatenbank über ein Netzwerk gespeichert wird, muss die Netzwerkfreigabe auch den Benutzer hier in der Registerkarte "Share Permissions" (Freigabeberechtigungen) mit Vollzugriff (SCHREIBEN) enthalten.

Standard: leer, <Lokal verwaltet>

Allgemeine (CAF)-Richtliniengruppe

Die allgemeine (CAF)-Richtliniengruppe enthält die folgenden Konfigurationsrichtlinien.

CAF: Präinitialisierungs-Skript

Gibt das auszuführende Skript an, wenn CAF gestartet wird und die Initialisierung gestartet wird. Das Skript wird ausgeführt, bevor die UUID überprüft wird und bevor Plug-ins gestartet werden.

CAF: Postinitialisierungs-Skript

Gibt das nach der Initialisierung von CAF auszuführende Skript an. Das Skript wird ausgeführt, nachdem alle Plug-ins gestartet wurden, jedoch bevor ihrer ersten Registrierung.

CAF: Zeitlimit (s) für Präinitialisierungs-Skript

Gibt die Zeit in Sekunden an, auf die CAF wartet, bevor das Präinitialisierungs-Skript beendet wird.

CAF: Zeitlimit (s) für das Postinitialisierungs-Skript

Gibt die Zeit in Sekunden an, auf die CAF wartet, bevor das Postinitialisierungs-Skript beendet wird.

CAF: Registrierung bei Start aktivieren

Gibt an, ob das allgemeine Anwendungsframework (CAF) sich sofort beim Start am Domänen-Manager registriert.

Standard: True

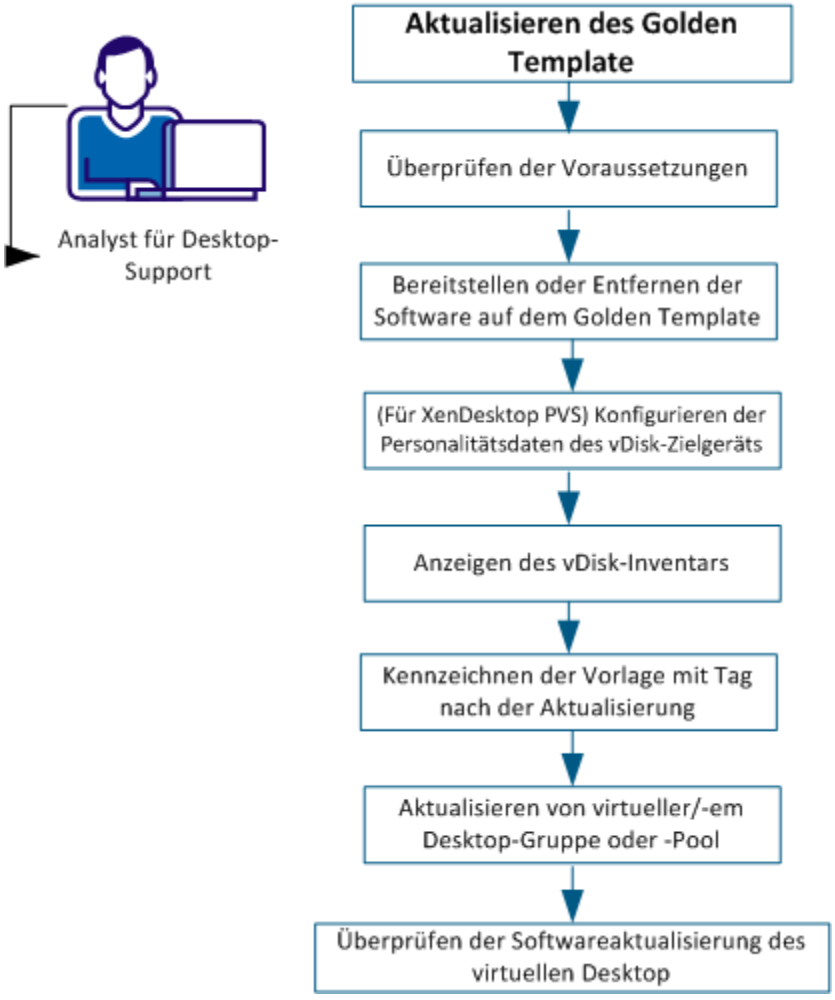
Wichtig! Diese Richtlinie muss lokal verwaltet werden, und zwar noch vor der Installation des CA DSM Agent VDI Support-Add-on Windows ENU-Pakets. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie aus dem Kontextmenü "Lokal verwaltet" aus.

Hinweis: Diese Richtlinie gilt nur für VMware View-basierte virtuelle Desktops und bei Verwendung des CA DSM Agent VDI Support-Add-on Windows ENU-Pakets von Versionen vor R12.5 SP1 Feature Pack 1.

Aktualisieren von Golden Templates

Als ein Desktop-Support-Analyst schließt Ihre Verantwortung auch das Aktualisieren von Golden Templates ein, wenn Sie Softwarepakete im Golden Template hinzufügen oder entfernen. Durch Aktualisierung des Golden Templates werden VMware View-Klone, Citrix PVS gestreamte virtuelle Desktops oder MCS-basierte virtuelle Desktops aktualisiert.

Das folgende Diagramm veranschaulicht die Schritte, die Sie ausführen, um Golden Templates zu aktualisieren:


Analyst für Desktop-Support
Aktualisieren des Golden Template
Überprüfen der Voraussetzungen
Bereitstellen oder Entfernen der Software auf dem Golden Template
(Für XenDesktop PVS) Konfigurieren der Personalitätsdaten des vDisk-Zielgeräts
Anzeigen des vDisk-Inventars
Kennzeichnen der Vorlage mit Tag nach der Aktualisierung
Aktualisieren von virtueller/-em Desktop-Gruppe oder -Pool
Überprüfen der Softwareaktualisierung des virtuellen Desktop

Führen Sie die folgenden Tasks aus, um das Golden Template zu aktualisieren:

1. Überprüfen der Voraussetzungen (siehe Seite 318)
2. Bereitstellen der Software im Golden Template (siehe Seite 318)
3. Konfigurieren der vDisk-Zielgerätepersönlichkeitsdaten (siehe Seite 319)
4. Anzeigen des vDisk-Inventars (siehe Seite 321)
5. Kennzeichnen der Vorlage nach der Aktualisierung (siehe Seite 322)
6. Aktualisieren der virtuellen Desktop-Gruppe oder des Pools (siehe Seite 323)
7. Überprüfen der Software-Aktualisierung des virtuellen Desktops (siehe Seite 324)

Überprüfen der Voraussetzungen

Um ein Golden Template zu aktualisieren, überprüfen Sie die folgenden Voraussetzungen:

- Überprüfen Sie, dass Sie bereits ein oder mehrere Golden Templates vorbereitet und bereitgestellt haben.
- Überprüfen Sie, ob der virtuelle Desktop-Agent auf dem Golden Template-Computer installiert ist.

  Hinweis: Ein umfassendes Wissen zu virtuellen Desktop-Lösungen wie VMware View und Citrix XenDesktop ist erforderlich.
- Überprüfen Sie, dass das Citrix PVS-Zielgerät installiert ist, wenn Sie Citrix vDisk-basierte virtuelle Desktops erstellen möchten.

Bereitstellen oder Entfernen von Software im Golden Template

Sie können Softwarepakete in einer der folgenden Weisen im Golden Template bereitstellen oder entfernen:

- Nehmen Sie die Änderungen direkt auf dem Golden Template-Computer vor. Diese Methode ist für VMware View und Citrix MCS anwendbar, die Snapshot-basiert sind.

- Aktualisieren Sie eine vDisk, die aus dem Golden Template erstellt wurde. Diese Methode ist für virtuelle Citrix XenDesktop-Desktops anwendbar, die von Citrix Provisioning Services gestreamt werden. Es gelten folgende Bedingungen:
  - Die vDisk muss im Privatmodus auf einem Computer gebootet werden, der die gleiche Konfiguration wie der Golden Template-Computer hat.
  - Das Zielgerät, das verwendet wird, um die vDisk im Privatmodus im Citrix-Bereitstellungsserver zu starten, wird mit Persönlichkeitsdaten zugewiesen, um anzuzeigen, dass die vDisk für die Vorlagenverwaltung gestartet wird. Weitere Informationen zu Persönlichkeitsdaten finden Sie unter Konfigurieren der vDisk-Zielgerätepersönlichkeitsdaten (siehe Seite 319).
  - Wenn Sie das erste Mal die vDisk im Privatmodus starten, wird die vDisk als eine verwaltete Entität in CA ITCM hinzugefügt. Sie können dann Pakete aus der vDisk mithilfe von Software Delivery bereitstellen oder entfernen.
  - Die vDisk wird als ein Computerdatensatz im DSM-Explorer unter "Alle Computer" mit der folgenden Namenskonvention angezeigt:

    <FarmName>-<StoreName>-<vDiskName>

    Wenn der Computerdatensatz nicht im DSM-Explorer gefunden wird, erhalten Sie weitere Informationen unter vDisk-Datensatz wurde nicht im DSM-Explorer gefunden.
  - Es wird jedes Mal der gleiche Computerdatensatz für die vDisk verwendet, wenn Sie die vDisk im Privatmodus auf einem Computer für Vorlagenverwaltung starten.
  - Wenn der Computer, der die vDisk im Privatmodus hostet, bereits ein verwalteter Computer in CA ITCM ist, erfolgen die Softwarebereitstellungen nur auf der vDisk und nicht auf dem Computer.

    Hinweis: Wenn der Computer mit der vDisk im Privatmodus gestartet wird, warten alle Softwarejobs, bis der Computer mit dem lokalen Laufwerk startet.

Hinweis: Sie können das Golden Template auch direkt aktualisieren, eine vDisk daraus erstellen oder eine vorhandene vDisk überschreiben, um die virtuellen Desktops zu aktualisieren.

(Für Xendesktop PVS) Konfigurieren der vDisk-Zielgerätepersönlichkeitsdaten

Konfigurieren Sie die vDisk-Zielgerätepersönlichkeitsdaten in der Bereitstellungsserver-Konsole, sodass CA ITCM die im Privatmodus gestartete vDisk als ein Golden Template betrachten kann.

Gehen Sie wie folgt vor:

1. Öffnen Sie das Dialogfeld "Eigenschaften" des Zielgeräts in Citrix Provisioning Services Console, dem die vDisk zugewiesen ist.
2. Klicken Sie auf die Registerkarte "Personality", und fügen Sie die folgenden Parameter hinzu:

   CA_DSM_GoldenTemplate

   Zeigt an, ob die vDisk ein Golden Template oder ein virtueller Desktop im Privatmodus ist. Legen Sie den Wert dieses Parameters auf "True" (Wahr) fest.

   ProvisioningServer

   Gibt die IP-Adresse oder den Hostnamen des Bereitstellungsservers an.

   ProvisioningServicesUser

   Gibt den Benutzernamen an, der Zugriff auf die Provisioning Services-Farm hat, oder den Benutzer, der angegeben wird, während eine Verbindung mit der Bereitstellungsserver-Konsole hergestellt wird. Verschlüsseln Sie den Benutzernamen mithilfe des Befehls "sd_acmd encrypt", und übergeben Sie den verschlüsselten Wert.

   ProvisioningServicesPassword

   Gibt das Kennwort des Provisioning Services-Benutzers an. Verschlüsseln Sie das Kennwort mithilfe des Befehls "sd_acmd encrypt", und übergeben Sie den verschlüsselten Wert.

   ProvisioningServerPort

   Gibt den Port des Bereitstellungsservers an, wo der SOAP-Service ausgeführt wird. Der Standardwert ist 54321.

   Hinweis: Übergeben Sie die Bereitstellungsserver-Parameter als Benutzerparameter im CA DSM-Agent VDI-Support-Add-on-Paket, während Sie den Vorlageinstallationsmodus auf das Golden Template übertragen. Verwenden Sie das folgende Format:

   ```
   /pvsserver:<server IP/Name> /pvsuser:<encrypted username> /pvspwd:<encrypted pwd> /portno:<portno>
   ```

3. Speichern Sie die Änderungen.

   Die vDisk-Zielgerätepersönlichkeitsdaten werden als Golden Template konfiguriert.

Anzeigen des vDisk-Inventars

Nachdem Sie die vDisk im Privatmodus gestartet haben, wird sie als eine verwaltete Entität in CA ITCM hinzugefügt. Hier ist ein Beispiel für Citrix XenDesktop.

Gehen Sie wie folgt vor: (in DSM-Explorer):

1. Navigieren Sie zu "Computer und Benutzer", "Alle Computer", "*vDisk-Name*", "Inventar", Knoten "System".

   vDisk-Name

   Gibt den vDisk-Namen im Format *FarmName-StoreName-vDisk.Name* an.

2. Wählen Sie den Unterordner "Vorlageneinstellungen" aus, um die Werte für die folgenden Attribute anzuzeigen:

   IsGoldenTemplate

   Zeigt an, ob ein Agent ein Golden Template (True) oder ein virtueller Desktop ist (False). Der Wert wird auf "True" (Wahr) gesetzt, wenn eine Master-vDisk oder ein Klon einer Master-vDisk im Privatmodus für die Vorlagenverwaltung gestartet wird.

   TemplateHostUUID

   Gibt die Host-UUID des Golden Templates an. Für eine Master-vDisk ist hostuuid das Golden Template und die Master-vDisk für geklonte vDisks.

   Weitere Informationen finden Sie unter Wie vDisk-Klone verarbeitet werden. (siehe Seite 324)

   TemplateName

   Gibt den Namen des Golden Templates an.

   TemplateTag

   Zeigt das Datum und Uhrzeit der letzten Tag-Kennzeichnung des Golden Templates an.

3. Klicken Sie auf den Vorlageverlauf-Knoten, um den Vorlageverlauf für die vDisk anzuzeigen. Sie können den Verlauf von Aktualisierungen am Golden Template sehen.

4. Klicken Sie auf "Virtualisierung", "Citrix XenvDisks".

   Farm, Speicher und Ort der vDisk werden angezeigt.

Gehen Sie wie folgt vor: (in der Webkonsole)

1. Navigieren Sie zu "Computer", "Inventar", "Erkanntes Inventar", und klicken Sie auf "Betriebssystem".
2. Klicken Sie auf der Registerkarte "More Details" auf "Vorlageneinstellungen", um die Werte für die Attribute IsGoldenTemplate, TemplateName, TemplateTag und TemplateHostUUID anzuzeigen.
3. Klicken Sie auf der Registerkarte "More Details" auf "Vorlageverlauf", um den Vorlageverlauf anzuzeigen.

Sie haben die Beziehungsinformationen und den Vorlageverlauf überprüft.

Kennzeichnen der Vorlage nach der Aktualisierung

Durch Kennzeichnen mit einem Tag können Sie die Version der Vorlage verfolgen, die von den virtuellen Desktops verwendet wird. Kennzeichnen Sie die Vorlage, um einen Vorlagetag zu generieren, und ordnen Sie die Klone ihrem übergeordneten Golden Template zu.

Gehen Sie wie folgt vor:

1. Ziehen Sie den Vorgang für die Tag-Vorlage vom CA DSM-Agent-Add-On-VDI-Paket zum Golden Template im DSM-Explorer.
2. Führen Sie *eine* der folgenden Aktionen aus, je nach virtueller Desktop-Lösung:
   - (Für auf Citrix PVS basiertes XenDesktop) Fahren Sie den Rechner herunter, sodass die Aktualisierungen auf der vDisk gespeichert werden.
   - (Für VMware View und Citrix MCS) Fahren Sie den virtuellen Rechner herunter, und erstellen Sie einen Snapshot.

     Diese Aktion ordnet den Snapshot dem Vorlage-Tag zu.

Aktualisieren der virtuellen Desktop-Gruppe oder des Pools

Aktualisieren Sie die virtuelle Desktop-Gruppe oder den Pool, die bzw. der das Golden Template verwendet, das Sie aktualisierten. Weitere Informationen zur Aktualisierung der virtuellen Desktop-Gruppe oder des Pools finden Sie in der VMware View- oder Citrix XenDesktop-Dokumentation. Nachdem die virtuelle Desktop-Gruppe oder der Pool aktualisiert worden ist, werden die Golden Template-Aktualisierungen beim nächsten Neustart an die virtuellen Desktops übertragen.

Weisen Sie die aktualisierte vDisk oder den Snapshot virtuellen Desktops zu, um die Golden Template-Aktualisierungen beim nächsten Neustart zu übertragen.

Gehen Sie wie folgt vor: (für VMware View)

1. Schließen Sie das Golden Template.
2. Fertigen Sie einen Snapshot des Golden Templates an.
3. Führen Sie mithilfe des neuen Snapshots eine Pool-Neuzusammenstellung durch.

Gehen Sie wie folgt vor: (für vDisk-basierte virtuelle Desktops)

1. Fahren Sie den vDisk-Computer herunter.
2. Entfernen Sie die vDisk-Zuweisung aus dem Computer.
3. Ändern Sie den vDisk-Modus zu Standard oder Differenz.
4. Weisen Sie die aktualisierte vDisk virtuellen Desktops zu.
5. Starten Sie die virtuellen Desktops neu; andernfalls treten die Änderungen erst in Kraft, wenn die virtuellen Desktops neu gestartet werden.

   Hinweis: Alternativ können Sie die aktualisierte vDisk den virtuellen Desktops entweder mithilfe der Automatik oder mithilfe der inkrementellen vDisk-Aktualisierungsfunktion von Citrix Provisioning Services zugewiesen werden.

Gehen Sie wie folgt vor: (für MCS-basierte virtuelle Desktops)

1. Schließen Sie das Golden Template.
2. Fertigen Sie einen Snapshot des Golden Templates an.
3. Aktualisieren Sie den Katalog "Pooled" mit dem neuen Snapshot.

Überprüfen der Software-Aktualisierung des virtuellen Desktops

Zeigen Sie die virtuelle Desktop-Software an, um zu überprüfen, ob die Aktualisierungen, die Sie am Golden Template vorgenommen haben, auf den virtuellen Desktops verfügbar sind.

Gehen Sie wie folgt vor:

1. Navigieren Sie zum Knoten "Computer und Benutzer", "Alle Computer", *Virtueller Desktop*, "Software", "Installierte Pakete".

   Überprüfen Sie im rechten Bereich, ob die Änderungen, die Sie am Golden Template oder an der vDisk vorgenommen haben, sich im virtuellen Desktop widerspiegeln.

Die Aktualisierungen am Golden Template sind vollständig.

Verwalten von vDisks und vDisk-Klonen

Als ein Desktop-Support-Analyst müssen Sie verstehen, wie CA ITCM die Beziehung zwischen der vDisk und ihren Klonen verarbeitet und verwaltet.

Dieses Szenario beschreibt, wie CA ITCM vDisks und Klone verarbeitet.

Wie vDisk-Klone verarbeitet werden

Sie können die vDisks kopieren oder klonen, um virtuelle Desktops bereitzustellen. vDisk-Kopien oder -Klone und ihre übergeordnete vDisk werden als separate Verwaltungsdatensätze in der MDB angezeigt. Die comstore-Werte von Bereitstellungsserver-Farm, Speicher, Standort, vDisk-Name unterscheiden eine übergeordnete vDisk von einer geklonten vDisk.

CA ITCM verwendet die folgenden Regeln, um vDisk-Klone zu identifizieren und einen separaten Verwaltungsdatensatz zu erstellen:

- Ein neuer Verwaltungsdatensatz wird in CA ITCM erstellt und der Agentenname ist im Format *FarmName-StoreName-vDisk*, wenn eine vDisk im Privatmodus für die Vorlagenverwaltung gestartet wird.
- Ein neuer Verwaltungsdatensatz wird für den Klon erstellt, wenn ein vDisk-Klon im Privatmodus für die Vorlagenverwaltung von einer anderen Farm gestartet wird.
- Ein neuer Verwaltungsdatensatz wird für die vDisk-Kopie erstellt, wenn der Klon von der gleichen Farm und einem anderen Speicher gestartet wird und die vDisk und ihr übergeordneter Name unterschiedlich sind.
- Ein neuer Verwaltungsdatensatz wird für die vDisk-Kopie anhand der folgenden Regel erstellt:
  - Die Klon-vDisk wird von der gleichen Farm und einem anderen Speicher gestartet
  - vDisk und ihr übergeordneter Name sind gleich
  - Der Standort, von dem die vDisk für die Vorlagenverwaltung gestartet wird, und ihre übergeordnete sind unterschiedlich

    Hinweis: Wenn der Standort der gleich wie bei der übergeordneten vDisk ist, wird der Administrator aufgefordert zu überprüfen, ob er einen Verwaltungsdatensatz in der MDB erstellen möchte oder den vorhandenen wieder verwenden will.
- Ein neuer Verwaltungsdatensatz wird anhand der folgenden Regel erstellt:
  - Farm und Speicher sind gleich
  - vDisk-Name wurde geändert
  - Übergeordnete vDisk ist Teil des Speichers
  - vDisk wird als Kopie gestartet

    Hinweis: Wenn die übergeordnete vDisk nicht Teil des Speichers ist, wird der Administrator aufgefordert zu überprüfen, ob er einen Verwaltungsdatensatz in der MDB erstellen möchte oder den vorhandenen wieder verwenden will.
- Ein vorhandener verwalteter Computerdatensatz wird wieder benutzt, wenn vDisk, Farm und Speichername gleich sind.

Anzeigen der Beziehung zwischen Golden Template, Master-vDisk und Klonen

Um die vDisk zu identifizieren, von der eine bestimmte vDisk abgeleitet wurde, erfasst CA ITCM das Inventar unter Vorlageneinstellungen und Vorlageverlauf.

Mithilfe dieser Inventarinformationen können Sie die unmittelbar übergeordnete einer bestimmten vDisk und den Verlauf von Änderungen an einer vDisk feststellen. Die Beziehung wird folgendermaßen identifiziert:

- Eine Master-vDisk verweist auf das Golden Template als übergeordnet.
- Wenn Sie einen Klon aus einer Master-vDisk erstellt haben, nachdem die Master-vDisk im Privatmodus gestartet wurde, verweist der Klon auf die Master-vDisk als übergeordnetes Element.
- Wenn Sie einen Klon aus einer Master-vDisk erstellt haben, bevor die Master-vDisk im Privatmodus gestartet wurde, gleicht der Klon der Master-vDisk und verweist auf das Golden Template als übergeordnet. Wenn weitere Klone von solchen vDisk-Klonen der Master-vDisk erstellt werden, verweisen alle Klone auf das Golden Template als übergeordnet.

Gehen Sie wie folgt vor: (in DSM-Explorer)

1. Navigieren Sie zu "Computer und Benutzer", "Alle Computer", "vDisk-Name", "Inventar", Ordner "System".
2. Wählen Sie den Unterordner "Vorlageneinstellungen" aus, um die Werte für die folgenden Attribute anzuzeigen:

   IsGoldenTemplate

   Zeigt an, ob der fragliche Agent ein Golden Template (True) oder ein virtueller Desktop ist (False). Der Wert ist "True" (Wahr) für die Master-vDisk und ihre Klone.

   TemplateHostUUID

   Gibt die Host-UUID des Golden Templates an. Für eine Master-vDisk wird die Host-UUID des Golden Templates angezeigt. Für geklonte vDisks unterscheidet sich die Host-UUID je nach den folgenden Faktoren:

   - Wenn der Klon aus erstellt wurde, nachdem die Master-vDisk im Privatmodus gestartet wurde, wird die Host-UUID der Master-vDisk angezeigt.
   - Wenn der Klon aus erstellt wurde, bevor die Master-vDisk im Privatmodus gestartet wurde, wird die Host-UUID des Golden Templates angezeigt.

   TemplateName

   Gibt den Namen des Golden Templates an.

   TemplateTag

   Zeigt Datum und Zeitstempel der Vorlage für das Golden Template oder die vDisk an, wenn die Vorlage mit einem Tag gekennzeichnet worden ist.
3. Wählen Sie den Vorlageverlaufs-Unterordner aus, um den Vorlageverlauf für den virtuellen Desktop oder die Vorlagen anzuzeigen, vorausgesetzt, dass die Vorlagen gekennzeichnet worden sind.

Gehen Sie wie folgt vor: (in der Webkonsole)

1. Navigieren Sie zur Seite "Computer", "Inventar", "Erkanntes Inventar".
2. Klicken Sie auf die Registerkarte "System", um den Wert des Attributs "Virtueller Rechner" anzuzeigen.
3. Klicken Sie auf der Registerkarte "More Details" auf "Vorlageneinstellungen", um die Werte für die Attribute IsGoldenTemplate, TemplateName, TemplateTag und TemplateHostUUID anzuzeigen.
4. Klicken Sie auf der Registerkarte "More Details" auf "Vorlageverlauf", um den Vorlageverlauf für den Klon anzuzeigen.

   Sie haben die Beziehungsinformationen und den Vorlageverlauf überprüft.

Verwalten von virtuellen Desktops von CA ITCM aus

Als ein Desktop-Support-Analyst schließt Ihre Verantwortung auch das Verwalten von virtuellen Desktops von CA ITCM aus ein. Das Verwalten von virtuellen Desktops umfasst das Bereitstellen von Software oder Patches für die virtuellen Desktops und Erfassen des Inventars von ihnen. Sie müssen auch wissen, wie und wann CA ITCM die Software auf den Desktops neu installiert.

Hinweis: Softwarepakete bereitstellen und Inventar von virtuellen Desktops erfassen erfolgt ähnlich wie die Softwarebereitstellung und Inventarerfassung auf anderen Computern in CA ITCM.

Implementierungshandbücher für virtuelle Desktops

Für Softwarepakete, die auf einzelnen virtuellen Desktops installiert sind und nicht auf dem Golden Template, sind folgende Einschränkungen und Anleitungen zu berücksichtigen:

- Pakete, die nicht auf dem Scalability-Server, wofür der Agent registriert ist, in der Softwarebibliothek durch Staging bereitgestellt sind, werden nicht erneut installiert.
- Die Neuinstallation wird für hinzugefügte Prozeduren mit neuen Dateien nicht unterstützt.
- Die Neuinstallation wird für den Benutzerprofile-Agenten nicht unterstützt, nur für den Computeragenten.
- Wenn ein virtueller Desktop mithilfe der Offline-Desktop-Funktion von VMware View ausgecheckt wird und ein Rollback erfolgt (Checkout wird demnach verworfen), verbleiben alle Änderungen am Softwarestatus in der Softwaredatenbank der Instanz. Beim Ausführen des Offline-RAC wird die Software neu installiert, da sie in der Statusdatenbank aufgezeichnet und während des Rollbacks nicht entfernt wurde. Daher muss die Software manuell deinstalliert werden, wenn Sie sie nicht benötigen.
- Das Senden von Software Delivery-Jobs mit den aktivierten Optionen "Neu starten"/"Abmelden"/"Herunterfahren" wird für nicht persistente virtuelle Desktops nicht unterstützt. Ein nicht persistenter Desktop ist nur solange an einen Benutzer gebunden, solange der Benutzer angemeldet ist. Bei der nächsten Anmeldung des Benutzers kann dem Benutzer ein anderer Desktop zugeordnet werden. Daher sind diese Optionen nicht logisch für diesen Fall.
- Pakete, die eine lange Übertragungszeit über das Netzwerk oder eine lange Installationszeit in Anspruch nehmen, müssen im Golden Template installiert werden und nicht auf dem einzelnen virtuellen Desktop. Ansonsten wird die Neuinstallation nicht akzeptabel.

- Virtualisierte Anwendungen können im Golden Template vorab durch Staging bereitgestellt werden und später mithilfe einer eigenständigen Installation an die einzelnen virtuellen Desktops verteilt werden. So lässt sich Ihre Netzwerkbandbreitenauslastung bei Neuzusammenstellungs-/Aktualisierungsvorgängen und während der Verwendung minimieren.
- Ein dem vorherigen Element ähnliches Ergebnis kann mithilfe der verwalteten Paketformate, wie SXP, PIF und MSI, mit einiger Recherche und möglicherweise einiger Optimierung erzielt werden. Beispielsweise stellt SXP einen Benutzerfilter bereit, der dem Paket ermöglicht, auf dem Golden Template installiert zu werden. Der Filter steht jedoch nur Benutzern der Klone zur Verfügung, die zu bestimmten lokalen oder Active Directory-Benutzergruppen gehören.
- Virtualisierte Anwendungen müssen auf einzelne virtuelle Desktops im Streaming-Modus verteilt werden. So lässt sich die Netzwerkbandbreitenauslastung bei Neuzusammenstellungs-/Aktualisierungsvorgängen minimieren, nicht aber während der Verwendung.
- Anwendungen, die ihre Konfiguration außerhalb des bzw. der umgeleiteten Benutzerprofils/Ordner speichern, behalten ihre Konfiguration nach der Neuinstallation nicht automatisch bei. Anwendungen, die ihre Konfiguration zurücksetzen und nicht als Bestandteil der Installation vererben, leiden unter diesem Problem.
- Wenn sowohl die Vorlage-Softwarestatusdatenbank als auch die Instanz-Softwarestatusdatenbank Datensätze derselben Software aufweisen, jedoch von unterschiedlichen Versionen, wird das Up- oder Downgrade weiterhin durch den Offline-RAC ausgeführt. Der Administrator ist für die entsprechende Konfiguration des Systems und die Verhinderung eines solchen Falls verantwortlich, insbesondere in Downgrade-Szenarien.
- Die DTS-Downloadmethode wird für den virtuellen Desktop-Agenten nicht unterstützt.
- Bei nicht persistenten Desktop-Pools werden Neuinstallationen nur abgeschlossen, wenn sich ein Benutzer anmeldet. Wenn sich der Benutzer von einem geklonten Desktop abmeldet, das Bestandteil eines mit der Option "Power off and delete virtual machine after first use" (Virtuelle Computer nach erster Verwendung ausschalten und löschen) in VMware View 4.0 erstellten nicht persistenten Desktop-Pools ist, dann befindet sich der geklonte Desktop im Status "Von RAC gesperrt", bis sich wieder ein Benutzer anmeldet. Bei VMware View 4.5 tritt die äquivalente Situation auf, wenn die Option "Delete or refresh desktop on logoff" (Desktop bei Abmeldung löschen oder aktualisieren) auf "Refresh Immediately" (Sofort aktualisieren) oder "Delete Immediately" (Sofort löschen) festgelegt wird. Daher sollten alle kritischen Patches als Bestandteil des Golden Template bereitgestellt werden und nicht als Bestandteil des Klons.

- Sie sollten den Benutzerprofilmodus für die Software Delivery-Funktion bei Vorhandensein verknüpfter virtueller Desktop-Klone deaktivieren.

  Benutzerprofile werden hier nicht benötigt, da eine 1:1-Beziehung zwischen dem Benutzer und dem virtuellen Desktop vorliegt. Das Aktivieren der Benutzerprofile verursacht eine zusätzliche Kommunikation zwischen dem Agenten und dem Scalability-Server, was sich auf die Gesamtskalierbarkeit auswirken kann.

Offline-RAC

Bei einem *Offline-RAC* handelt es sich um einen RAC-Task (Neuinstallation nach Absturz, Reinstall After Crash), der nicht durch den Manager, sondern durch den Agent gesteuert wird. Virtuelle Desktops werden häufig *erneut erstellt*, das heißt, wenn das Golden Template aktualisiert und die Festplatte zurückgesetzt wird, werden alle Änderungen am virtuellen Desktop seit der vorherigen Zurücksetzung effektiv ungültig gemacht. Bei virtuellen Desktops ist nicht der Manager, sondern der Agent für die Erstellung des RAC-Jobcontainers verantwortlich. Bei einer Datenträgerzurücksetzung initiiert der Agent einen Offline-RAC, um sämtliche Software wiederherzustellen, die für den Agent bereitgestellt wurde.

Für den Offline-RAC wurde der Software Delivery-Agent mit einer Dateisystem-basierten Softwarestatusdatenbank erweitert. Diese Datenbank enthält die folgenden Informationen über jedes installierte Softwarepaket:

- Die zum Installieren der Software verwendete Prozedur.
- Installationsnachbereitungsaktivierungs- oder -konfigurationsprozeduren nur für das Computerziel des Agenten.
- Sämtliche jobspezifischen Informationen, beispielsweise Benutzerparameter.

Diese Softwarestatusdatenbank wird vom Software Delivery-Agenten verwaltet und jedes Mal aktualisiert, wenn ein Softwarejob ausgeführt wird. Nach einer erfolgreichen Deinstallation werden die Datensätze für dieses bestimmte Softwarepaket entfernt. Wenn die Option aktiviert ist, spiegelt die Softwarestatusdatenbank immer den aktuellen Software Delivery-Status des Agenten wider.

Darüber hinaus erbt die Softwarestatusdatenbank auch den Installationsverlauf des Golden Template, auf dem der virtuelle Desktop basiert. Die Softwarestatusdatenbank besteht aus zwei Teilen, einem Teil für das Golden Template und einem Teil für die Verwendung der geklonten Instanz. Der Vorlagenteil der Softwarestatusdatenbank wird auf der Systemfestplatte der Golden Template gespeichert. Alle auf die Golden Template gerichteten Softwarejobs verwenden nur diese Datenbank. Wenn der virtuelle Desktop geklont wird, verwendet der entsprechende Agent nur die Instanz-Softwarestatusdatenbank, um den Status zu verfolgen.

Da die Systemfestplatte eines geklonten virtuellen Desktops während einer Neuzusammensetzung oder Aktualisierung gelöscht wird, kann die Instanz-Softwarestatusdatenbank nicht auf der Festplatte gespeichert werden. Diese Datenbank muss an einem anderen Ort gespeichert werden, der von einer allgemeinen Konfigurationsrichtlinie gesteuert wird - z. B. auf dem Datenträger für Benutzerdaten eines Klons, der mit VMware View verknüpft ist, oder auf einem Dateiserver, auf den von einem virtuellen Desktop aus zugegriffen werden kann.

Wichtig! Administratoren müssen sicherstellen, dass beim standardmäßigen Software-Jobmanagement und beim Durchführen einer Offline-Installation jederzeit der Zugriff auf die Softwarestatusdatenbank möglich ist, wenn sich die Instanz-Softwaredatenbank auf einer Netzwerkfreigabe befindet.

Weitere Informationen:

Richtliniengruppe "Software Delivery (Agent)" (siehe Seite 310)

Status der Neuinstallation

Nach dem Abschluss des Neuinstallationsprozesses wird dem Domänen-Manager jeder erfolgreiche oder fehlerhafte Job gemeldet. Der Status wird zudem im Dialogfeld "Software Delivery - Jobprüfung" des Agenten angezeigt, wenn die Offline-Neuinstallation ausgeführt wird.

Treten bei einem Job Fehler auf oder wenn einige Jobs aufgrund anderer Einstellungen (wie "Aus RAC ausschließen") nicht ausgeführt werden können, ist das Dialogfeld "Software Delivery - Jobprüfung" konfiguriert, geöffnet zu bleiben, bis der Benutzer es explizit schließt. Diese Software Delivery-Agent-RAC-Richtlinie ist konfigurierbar und kann deaktiviert werden. Im Falle eines Fehlers beim Initiieren einer Offline-Neuinstallation, beispielsweise im Falle einer ungültigen Downloadmethode oder bei einem Versuch, einem Legacy-Scalability-Server eine Meldung zu erteilen, wird dieser Fehler ebenfalls im Dialogfeld "Software Delivery - Jobprüfung" aufgeführt. Wenn der Zugriff auf den Scalability-Server aufgrund verschiedener Gründe nicht möglich ist, stehen dem Endbenutzer Optionen zur Verfügung, um die Neuinstallation zu wiederholen, zu verschieben oder abzubrechen.

Computereigenschaften

Die RAC-Richtlinieneinstellung der Agentenrichtlinie wird standardmäßig auf die Registerkarte "Software Delivery" des Dialogfelds "Computereigenschaften" festgelegt. Das RAC-Richtlinienfeld wird deaktiviert, wenn die Agentenrichtlinie auf "Wahr" festgelegt ist und Sie die Einstellung nicht ändern können.

Die DTS-Downloadmethode wird während des Offline-RAC-Vorgangs für virtuelle Desktops nicht unterstützt. Daher wird diese Option in der Drop-down-Liste "Download-Methode" nicht angezeigt.

Entsperren von virtuellen Computern

Nachdem der Agent die Software neu installiert hat, sendet er dem Scalability-Server eine Benachrichtigung über den Offline-RAC-Abschluss, welcher ihn wiederum an den Manager sendet. Nachdem der Manager diese Benachrichtigung empfangen hat, entsperrt er den virtuellen Computer vom Offline-RAC.

Wenn der Agent die Software neu installiert hat, dem Scalability-Server jedoch keine Benachrichtigung über den Offline-RAC-Abschluss senden konnte, können Sie die Entsperrung des virtuellen Computers erzwingen. Wenn der Agent beispielsweise die Benachrichtigung nicht senden kann, sofern der Server in diesem Augenblick nicht verfügbar war, können Sie den virtuellen Computer entsperren.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie im DSM-Explorer zu "Computer und Benutzer" und zum Ordner "Alle Computer".
2. Klicken Sie mit der rechten Maustaste auf das entsprechende Asset im dazugehörigen Bereich "Alle Computer".
3. Wählen Sie im angezeigten Kontextmenü den Befehl "Ausstehende RAC-Sperre löschen" aus.

   Hinweis: Dieser neue Befehl ist nur verfügbar, wenn die Spalte "SD-Status" anzeigt, dass mindestens ein virtueller Computer durch RAC gesperrt ist. Andernfalls wird der Befehl deaktiviert. Des Weiteren wird dieser Befehl nicht für einen normalen Computer aktiviert, der in den Status "Von RAC gesperrt" wechselt.

   Das ausgewählte Asset wird entsperrt.

Löschen der virtuellen Computer im DSM-Explorer

Wenn nach der Erstellung von Klonen ein Golden Template von einem Domänen-Manager zum nächsten verschoben wird, wird das Golden Template auf Grundlage der standardmäßigen Verschiebungsfunktionalität verschoben. Wenn auf Grundlage dieses Golden Templates erstellte Klone neu zusammengesetzt werden, erteilen die Klone dem neuen Domänen-Manager automatisch eine Meldung in einem Bericht. Daher muss für einen neu zusammengesetzten Klon nichts verschoben werden, da sein gesamter Installationsverlauf mithilfe des Offline-RAC erneut erstellt wird.

Um veraltete Klone zu bereinigen, die nur noch aus Berichtszwecken verwendet, jedoch nicht mehr länger vom vorherigen Domänen-Manager verwaltet werden, müssen Sie alle verschobenen Klone dieses Managers nach der Neuzusammensetzung des Golden Templates manuell löschen.

Wenn das Benennungsmuster geändert und ein bestimmter virtueller Computer mithilfe von VMware View gelöscht wird, wird ebenfalls ein neuer virtueller Computer mit einem neuen Namen erstellt. Löschen Sie in diesem Fall den virtuellen Computer aus dem DSM-Explorer.

Softwareprozeduren

Im Software Delivery-System können Sie derzeit RAC für einzelne Softwareprozeduren aktivieren oder deaktivieren. Wenn eine Elementprozedur nicht als Teil des RAC-Prozesses ausgeführt werden soll, können Sie die Option "Aus RAC ausschließen" im Dialogfeld "Eigenschaften" der tatsächlichen Prozedur auswählen. Diese Option ermöglicht es Ihnen, veraltete Pakete oder Patches aus RAC auszuschließen.

Die Funktionalität "Aus RAC ausschließen" wurde erweitert, um den Offline-RAC zu unterstützen. Während einer Offline-Neuinstallation ist die Einstellung "Aus RAC ausschließen" im Dialogfeld "Eigenschaften" für jede Softwareprozedur aktiviert, und die Prozedur wird nicht ausgeführt, wenn die Prozedur ausgeschlossen ist.

Ein Beispiel ist, bei dem ein einzelner Patch möglicherweise erforderlich ist, um ein kritisches Sicherheitsproblem zu lösen, das Ihre virtuellen Desktops einbezieht, ohne sie neu zusammensetzen zu müssen. Sobald die Zusammensetzung erfolgt ist, weist die neue Version des Golden Templates jedoch alle angewandten Patches auf, wodurch das Neuinstallieren dieses Patches sich erübrigt.

Anwenden von Sicherheits-Patches auf virtuellen Desktops

Um die Software-Neuinstallation auf virtuellen Desktops auszulösen, die Änderungen nach der Benutzerabmeldung oder einem Neustart nicht persistent beibehalten, führt CA ITCM den Offline-RAC-Prozess aus. Wenn der Benutzer sich das nächste Mal beim virtuellen Desktop anmeldet, installiert Offline-RAC die Software und Patches neu, die der Benutzer vor seiner Abmeldung oder dem Neustart installiert hatte.

(Optional) Konfigurieren von Patch Manager zur Handhabung der Patch-Bereitstellung während RAC oder auf neu zusammenstellbaren virtuellen Desktops

Standardmäßig wird die Patch-Bereitstellung während RAC ausgeschlossen, weil die Patches erneut bereitgestellt werden, ohne die Reihenfolge der Ersetzungen oder Rollouts zu berücksichtigen. Dieses Verhalten kann zu einem unerwarteten Ergebnis führen. Auf ähnliche Weise werden auf die Blacklist (schwarze Liste) gesetzte Ziele ebenfalls während der Patch-Bereitstellung ausgeschlossen.

Neu zusammenstellbare virtuelle Desktops gehören standardmäßig zu den auf die schwarze Liste gesetzten Computern. Die Standardeinstellungen für das Ausschließen von RAC und das Ignorieren von Computern auf der schwarzen Liste sind ideal, um die Patch-Bereitstellung zu verarbeiten. Sie können die Einstellungen ändern, um das Standardverhalten zu ändern.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA Patch Manager an.
2. Navigieren Sie zu "Administration", "Konfiguration", "Systemeinstellungen", "DSM", "Optionen".

   Die Konfigurationsoptionen werden angezeigt.
3. Ändern Sie die folgenden Parameter nach Bedarf:

   Von RAC ausschließen

   Schließt die Patch-Bereitstellung während eines RAC-Prozesses aus. Deaktivieren Sie diese Option, um während RAC Patches bereitzustellen. Die Patches werden erneut bereitgestellt, ohne die Reihenfolge der Ersetzungen oder Rollouts zu berücksichtigen, und können daher zu einem unerwarteten Ergebnis führen.

   Auf die Schwarze Liste gesetzte Computer bei der Bereitstellung ignorieren

   Gibt die Standardoption an, wenn auf die schwarze Liste gesetzte Ziele während der Patch-Bereitstellung zur ausgewählten Zieleliste hinzugefügt werden. Deaktivieren Sie diese Option, um nur die ausgewählten Ziele von der schwarzen Liste für die Patch-Bereitstellung einzuschließen. Sie können diese Option auch für individuelle Bereitstellungen ändern. Um auf die schwarze Liste gesetzte Ziele immer zu ignorieren, außer wenn anders angegeben, lassen Sie diese Option aktiviert.

   Auf die Schwarze Liste gesetzte Computer in der Richtlinie ignorieren

   Gibt an, dass die auf die schwarze Liste gesetzten Ziele während der Richtlinienauswertung ignoriert werden sollen. Wenn diese Option ausgewählt ist, wird die UPM-Blacklist-Abfrage zu den UPM-Richtlinienabfragen hinzugefügt.

   Eine Abfrage der schwarzen Liste ruft eine Liste von Computern ab, die von der Patch-Bereitstellung ausgeschlossen werden. Standardmäßig wird der blacklistQuery-Parameter auf die Abfrage "UPM–Blacklisted Computers" (UPM-Abfrage für die schwarze Liste) gesetzt. Diese Abfrage ist mit der Abfrage "Recomposable Computers" (Abfrage für neu zusammenstellbare Computer) verbunden, die neu zusammenstellbare Desktops abruft, die auf einem Inventarelement basieren. Das Inventarelement IsRecomposable befindet sich unter "Inventar", "System", "Vorlageneinstellungen". Zusätzlich zu den neu zusammenstellbaren Desktops können Sie auch Computer in die Abfrage "UPM–Blacklisted Computers" einschließen oder eine Abfrage erstellen, um solche Computer auszuschließen. Stellen Sie sicher, dass die neue Abfrage die Abfrage "Recomposable Computers" einschließt. Wenn Sie eine Abfrage für Computer auf der schwarzen Liste erstellen, geben Sie den Namen der Abfrage im Abrageparameter für die schwarze Liste an.

   Hinweis: Um die vorhandenen UPM-Richtlinien und Pakete automatisch zu aktualisieren, überprüfen Sie, dass Sie ein Upgrade für sie durchgeführt haben. Weitere Informationen zum Upgrade finden Sie im Thema Aktualisieren von Patch Manager-Paketen und -Richtlinien.

4. Speichern Sie die Einstellungen.

   Patch Management ist konfiguriert, um RAC und Computer auf der schwarzen Liste während der Patch-Bereitstellung zu verarbeiten.

Anwenden von Patches auf vDisk oder Golden Templates

Das Anwenden von Sicherheits-Patches auf vDisk oder Golden Templates stellt sicher, dass alle virtuellen Desktops die notwendigen Sicherheits-Patches installiert haben. Um den Patch auf vDisk oder ein Golden Template anzuwenden, folgen Sie der Anleitung unter "Aktualisieren von Golden Templates".

Anwenden von Patches auf Ziele auf der schwarzen Liste oder neu zusammenstellbare Desktops

Standardmäßig gehören neu zusammenstellbare Desktops zu den auf die schwarze Liste gesetzten Zielen, und alle Ziele auf der schwarzen Liste werden aus der Patch-Bereitstellung ausgeschlossen. Allerdings können Sie den Patch auf Ziele auf der schwarzen Liste anwenden, wenn es erforderlich ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA Patch Manager an und klicken Sie auf den Patch, den Sie auf die auf die schwarze Liste gesetzten Ziele anwenden möchten.
2. Klicken Sie auf der Seite "Patch-Details" auf "Patch bereitstellen".
3. Wählen Sie die Gruppe aus, die Blacklist-Ziele enthält, oder wählen Sie individuelle Ziele auf der schwarzen Liste aus, und fügen Sie sie dem angrenzenden Bereich "Ausgewählte Ziele" hinzu.

   Die Liste der auf die schwarze Liste gesetzten Ziele in der ausgewählten Gruppe oder die Ziele werden im Bereich "Auf die Schwarze Liste gesetzte Ziele" angezeigt.
4. Wählen Sie die Ziele, auf die Sie den Patch anwenden möchten, aus dem Bereich "Auf die Schwarze Liste gesetzte Ziele" aus. Fügen Sie diese Ziele dem angrenzenden Bereich "Ausgewählte Ziele" hinzu. Klicken Sie auf "Weiter".
5. Geben Sie den Bereitstellungsablaufplan an. Klicken Sie auf "Weiter".
6. Deaktivieren Sie die Option "Ignore Blacklisted computers in Deployment" (Auf die Schwarze Liste gesetzte Computer bei der Bereitstellung ignorieren). Klicken Sie auf "Fertig stellen".

   Die Patch-Bereitstellung auf den ausgewählten Zielen beginnt zur geplanten Zeit.

Anzeige des VDI-Inventars

Inventarinformationen werden für das Golden Template und die virtuellen Desktops mit unterschiedlichen Werten erfasst. Diese zeigen auf, ob ein virtueller Computer eine Vorlage oder ein Klon ist.

Gehen Sie wie folgt vor:

1. Navigieren Sie im DSM-Explorer zum Knoten "Computer und Benutzer", "Alle Computer", "Computername", "Inventar", "Betriebssystem".

   Zeigen Sie den Bereich "Betriebssystem" an.

2. Überprüfen Sie den Wert Attributs für den virtuellen Computer.

   Gibt an, ob der Computer ein virtueller Computer ist.

3. Wählen Sie "Vorlageneinstellungen" aus.

   Zeigt die folgenden Attribute an:

   IsGoldenTemplate

   Gibt an, ob ein virtueller Computer ein Golden Image (Wahr) oder ein Klon (Falsch) ist.

   Neu zusammensetzbar

   Gibt an, ob ein virtueller Desktop neu zusammensetzbar ist.

   TemplateHostUUID

   (Nur Klone) Gibt die Host-UUID des Golden Templates an.

   TemplateName

   (Nur Klone) Gibt den Namen des Golden Templates an.

   TemplateTag

   (Nur Klone) Gibt Datum und Uhrzeit des markierten Vorlagen-Snapshots an.

4. Vorlagenverlauf auswählen

   Zeigt den Vorlagenverlauf für den Klon an, wenn die Snapshots markiert sind.

5. Navigieren Sie zum Anzeigen des erfassten Virtualisierungsinventars zum Knoten "Computer und Benutzer", "Alle Computer", "Computername", "Inventar", "Virtualisierung".

   Zeigt die Desktop-Virtualisierungstechnologie an, die der Computer verwendet.

6. Erweitern Sie den Knoten "Virtualisierung", und wählen Sie Folgendes aus:

   VMware View

   Zeigt Pool-Namen und Agentenversion an.

   Konfiguration von Citrix XenDesktop

   Zeigt die Citrix-Farm, Gruppe, Lizenzierung und Produktinformationen an.

Hinweis: Wie andere Inventardaten können Sie auch das Virtualisierungsinventar verwenden, um Abfragen und Berichte zu erstellen.

Abfragen und Berichterstellung

Um die Abfrage und Berichterstellung auf Vorlagendesktops zusätzlich zu einzelnen Desktops zu unterstützen, die auf diesen Vorlagen basieren, wurde das grundlegende Hardwareinventar mit den folgenden Attributen und Werten erweitert:

IsGoldenTemplate

Boolescher Wert

Basiert auf TemplateName

Zeichenfolge

Basiert auf TemplateVersion

Ganzzahl

Basiert auf TemplateHostUUID

Zeichenfolge

Diese Attribute werden im Bereich "Alle Computer", *Computername*, "Inventar", "Betriebssystem" im DSM-Explorer angezeigt.

Änderungen am Abfrage-Designer

Beim Erstellen einer Abfrage stehen Ihnen nun zusätzliche Argumente für die Berichterstellung auf Computern mit einem Status des Offline-RAC zur Verfügung. Vordefinierte Abfragen wurden zusätzlich für den VDI-Support hinzugefügt.

- Für computerbasierte Abfragen wurde im Dialogfeld des Abfrage-Designers "Auswählen" der Drop-down-Liste "RAC-Richtlinie" ein Wert von "Offline" hinzugefügt.
- Dem Knoten "Abfragen" im DSM-Explorer wurden zwei vordefinierte VDI-Support-Abfragen, "Alle Golden Templates" und "Alle Klone von Golden Templates" hinzugefügt.

Änderungen am DSM-Reporter

Die folgenden vordefinierten Berichtsvorlagen für den VDI-Support wurden dem DSM-Reporter hinzugefügt:

- Alle Golden Templates
- Alle Klone von Golden Templates

Nachdem eine Berichtsvorlage ausgeführt und das Inventar erfasst wurde, listen diese Berichte alle entdeckten Golden Templates und ihre entsprechenden virtuellen Desktops auf.

Ausschließen von Golden Images durch den Assistenten für veraltete Assets

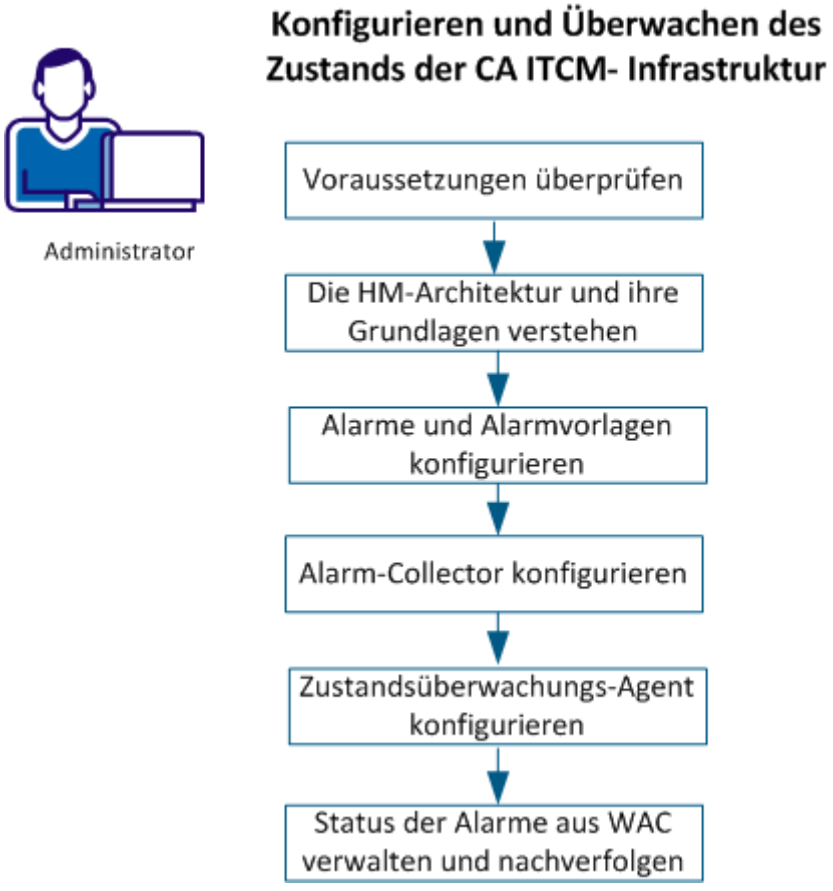
Der Assistent für veraltete Assets hilft Ihnen dabei, alte und nicht verwendete Computer und Benutzer nachzuverfolgen und optional zu entfernen. Da Golden Templates sich in puncto Logik von normalen Computern und deren Benutzern unterscheiden, wurden sie aus den Ergebnissätzen der durch den Assistenten generierten veralteten Asset-Abfragen ausgeschlossen. Eine mit einer vorherigen Version von CA IT Client Manager erstellte veraltete Asset-Abfrage schließt Golden Templates und die zugehörigen Benutzer nicht aus. Ersetzen Sie daher vorhandene veraltete Asset-Abfragen, um sicherzustellen, dass Golden Templates aus den Ergebnissätzen ausgeschlossen werden.

Kapitel 9: Konfigurieren und Überwachen des CA ITCM-Infrastrukturzustands

Als Administrator sind Sie auch für das Verwalten des CA ITCM-Komponentenzustands verantwortlich. Die Funktion "Zustandsüberwachung" bietet einen Zustandsanzeigemechanismus:

- Zum Definieren der CA ITCM-Zustandsbedingungen
- Zur regelmäßigen Überwachung der Infrastruktur
- Zum Auslösen eines Alarms, wenn eine definierte Bedingung festgestellt wird
- Zum Benachrichtigen des Administrators per E-Mail, zum Auslösen einer SNMP-Trap und zum Schreiben in die Windows-/CCS-Ereignisprotokolle.

Verwenden Sie die HM-Funktion, um die CA ITCM-Verfügbarkeit und Flexibilität zu verbessern. Die folgende Abbildung fasst den HM-Prozess zusammen:


Konfigurieren und Überwachen des Zustands der CA ITCM- Infrastruktur
Administrator
Voraussetzungen überprüfen
Die HM-Architektur und ihre Grundlagen verstehen
Alarme und Alarmvorlagen konfigurieren
Alarm-Collector konfigurieren
Zustandsüberwachungs-Agent konfigurieren
Status der Alarme aus WAC verwalten und nachverfolgen

Sie können die folgenden Tasks ausführen:

Konfigurieren von Alarmen

Konfigurieren Sie die verfügbaren Alarme oder definieren Sie neue Alarme.

Konfigurieren von Alarm-Aktionen

Konfigurieren Sie Alarm-Aktionen, wie das Senden von E-Mails, das Auslösen von SNMP-Traps sowie das Schreiben in das System und CCS-Ereignisprotokoll.

Verwalten von Alarmen

Sie können die Alarme über WAC anzeigen, verfolgen, nachverfolgen und löschen.

Dieses Kapitel enthält folgende Themen:

Überprüfen der Voraussetzungen (siehe Seite 342)
Verstehen der HM-Architektur und -Grundlagen (siehe Seite 343)
Konfigurieren von Alarmen und Alarmvorlagen (siehe Seite 348)
Alarm-Collector konfigurieren (siehe Seite 356)
Konfigurieren des Systemüberwachungs-Agenten (siehe Seite 364)
Verwalten und Verfolgen des Status von Alarmen von WAC (siehe Seite 369)

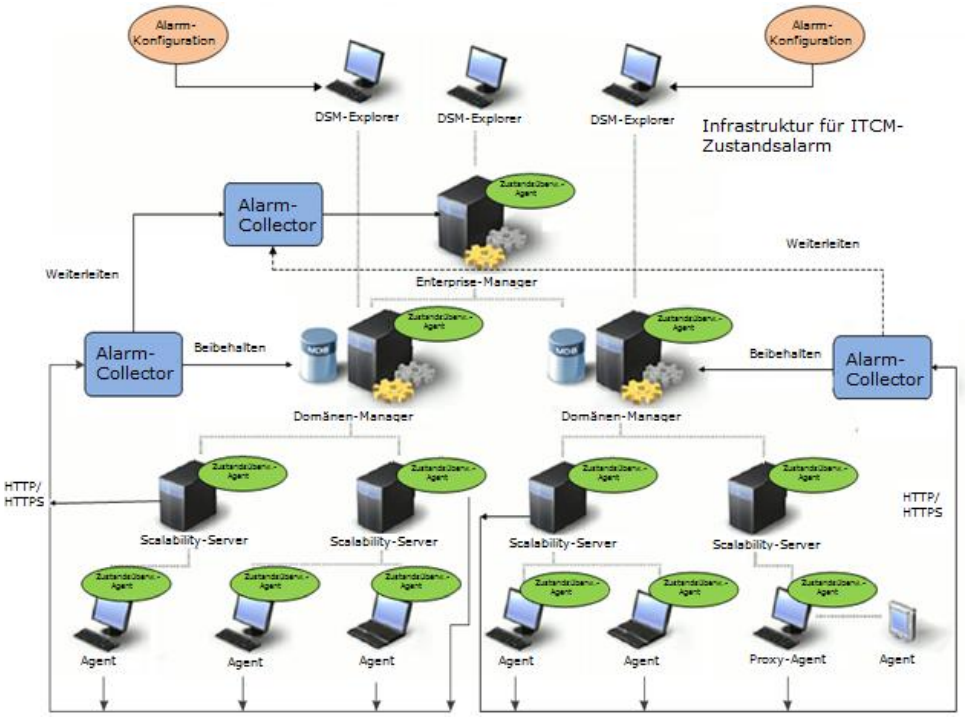
Überprüfen der Voraussetzungen

Vor dem Konfigurieren und Überwachen von HM-Alarmen muss Folgendes gewährleistet sein:

- Sie müssen mit der CA ITCM-Infrastruktur vertraut sein
- Sie müssen die HM-Architektur und -Grundlagen verstehen
- Sie müssen die vorhandene Infrastruktur mit CA ITCM Version 12.8 aktualisieren
- Installieren Sie den Alarm-Collector.

Verstehen der HM-Architektur und -Grundlagen

Das folgende Diagramm zeigt die Komponenten der HM-Funktion und wie sie zur Überwachung des Zustands von CA ITCM interagieren:



Weitere Informationen über die HM-Grundlagen finden Sie unter

- Alarme und Alarmvorlagen (siehe Seite 344)
- Systemüberwachungskomponenten (siehe Seite 345)
- Externer Prozess-Manager (CAF-Plug-in) (siehe Seite 347)

Alarme und Alarmvorlagen

Die HM-Funktion überwacht die folgenden Alarmtypen:

Parametrisierte Alarme (Alarmvorlagen):

Unterstützt zusätzliche Parameter als Teil der Alarmdefinition. Sie können Alarmeigenschaften, wie die Überwachungshäufigkeit, den Grenzwert und die Relevanz, auf Grundlage der für diese Parameter festgelegten Werte anpassen. Das Definieren und Konfigurieren parametrisierter Alarme wird über "Alarm-Vorlagen" unterstützt.

Eine Alarmvorlage enthält eine Standarddefinition eines parametrisierten Alarms mit einer Liste der unterstützten Parameter. Verwenden Sie die Vorlage als Grundlage für einen oder mehrere Alarme mit unterschiedlichen Parameterwerten und zugehörigen Konfigurationen.

Nichtparametrisierte oder einfache Alarme (Alarme):

Unterstützt keine zusätzlichen Parameter. Verwenden Sie die Alarmeigenschaften, wie im System definiert.

Die HM-Funktion bietet standardmäßig Alarmvorlagen und Alarme. Sie können angepasste Vorlagen und Alarme im Domänen-Manager-Skript begründen. Eine Liste mit Alarmen und Alarmvorlagen finden Sie in der Benutzeroberfläche.

Systemüberwachungskomponenten

Die HM-Funktion führt die folgenden Komponenten ein:

HM-Agent:

Ein persistentes Modul, das mit dem allgemeinen Agenten installiert wird und sich auf allen Stufen der CA ITCM-Infrastruktur befindet.

- Er interpretiert die Alarmkonfiguration auf den Agenten, führt regelmäßige Überwachungen hinsichtlich des Auftretens der Alarmbedingungen durch und benachrichtigt den Administrator, wenn die Zustandsbedingungen erkannt werden.

  Hinweis: Die Alarmüberwachung ist standardmäßig deaktiviert. Wenden Sie zum Aktivieren der Systemüberwachung eine Konfigurationsrichtlinie an.

- Geben Sie die folgenden Befehlszeilenoptionen für die Interaktion an:

  `hmagent start`

  Startet den HM-Agenten.

  `hmagent stop`

  Hält den HM-Agenten an.

  `hmagent status`

  Zeigt an, ob der Agent ausgeführt wird und die Systemüberwachung aktiviert ist.

- Der HM-Agent ist ein Service auf Windows-Plattformen und ein Daemon auf Linux-/UNIX-Plattformen.

Alarm-Collector:

Der Alarm-Collector besteht aus folgenden Modulen:

Webmodul

Empfängt die Alarme vom HM-Agenten und kopiert sie in einen konfigurierten Ordner.

Permanentes Modul

Überwacht den konfigurierten Ordner und verarbeitet neue Alarme gemäß der konfigurierten Alarm-Collector-Rolle. Weitere Informationen finden Sie unter Alarm-Collector konfigurieren (siehe Seite 356).

Der Alarm-Collector weist folgende Anforderungen auf:

- Der Alarm-Collector wird nur durch Windows unterstützt.
- Die IIS-Installation ist obligatorisch.
- Stellen Sie sicher, dass die verfügbaren ISAPI-Erweiterungen und -Filter unter der Option "Anwendungsentwicklung" installiert werden.
- In Abhängigkeit des DB-Typs, für den der Alarm-Collector den Alarm persistiert, muss der 32-Bit-SQL- oder der Oracle-Client installiert sein.

Die Webmodulanwendung hostet HM-Webservices auf IIS. Dieser Webservice ist unabhängig von der vorhandenen CA ITCM-Webservices-Funktion und wird in einem getrennten Anwendungspool ausgeführt.

Der Administrator kann den Status des Alarm-Collector-Prozesses von der unterstützten Befehlszeile starten, anhalten und abfragen. Der Alarm-Collector unterstützt die Befehlszeilenoptionen, ähnlich wie der HM-Agent.

Alarme auf WAC:

Der DSM-Explorer zeigt eine Benachrichtigung an, wenn neue Alarme ausgelöst werden. Die Benachrichtigung enthält einen Hyperlink, der WAC startet und zur Seite "Alarme" navigiert, wenn die vereinheitlichte Anmeldung für WAC aktiviert ist. Wenn die vereinheitlichte Anmeldung nicht aktiviert ist, geben Sie die entsprechenden Benutzeranmeldeinformationen an, um zur Seite "Alarme" zu navigieren.

Externer Prozess-Manager (CAF-Plug-in)

Dieses Plug-in (mit dem Namen cfProcessManager) verwaltet externe Prozesse, beispielsweise den HM-Agenten und den Alarm-Collector. Die Plug-in-Funktionalität ähnelt CAF, wobei CAF die CA ITCM-konformen Plug-ins verwaltet, während der Prozess-Manager externe Prozesse verwaltet, die keine CAF-Plug-ins darstellen.

Die externen Prozesse, die cfProcessManager verwaltet, unterstützen die normalen CAF-Plug-in-Eigenschaften wie *Maxinstances, Maxrestarts, Restartifdied, Enabled* und *Maxrestarttime.* Das Verhalten dieser Eigenschaften ähnelt dem von CAF-Plug-ins.

Die folgenden zusätzlichen Eigenschaften werden unterstützt:

Startwithcaf

Definiert den beim Start von CAF zu startenden Prozess.

Standard: Starten Sie nicht mit CAF.

Stopwithcaf

Definiert den beim Anhalten von CAF anzuhaltenden Prozess.

Standard: Halten Sie nicht mit CAF an.

Commandline

Zeigt die Befehlszeile des Prozesses an.

Startcmd

Definiert den Startbefehl. Standard: Start.

Stopcmd

Definiert den Befehl zum Anhalten. Standard: Anhalten.

Statuscmd

Definiert den Statusbefehl. Standard: Status.

Hinweis: Starten Sie "cfProcessManager" neu, wenn Sie die obigen Einstellungen ändern.

Eine neue */EXT*-Option wurde für die CAF-Befehle zum Starten und Anhalten eingeführt.

Caf start /EXT

Startet alle Plug-ins und die aktivierten externen Prozesse, die dieser Prozess-Manager verwaltet.

Caf stop /EXT

Hält alle Plug-ins und die aktivierten externen Prozesse an, die dieser Prozess-Manager verwaltet.

Der Befehl **Caf status cfProcessManager** zeigt den Status der externen Prozesse.

Konfigurieren von Alarmen und Alarmvorlagen

Sie können den Zustand von CA ITCM-Komponenten, beispielsweise Enterprise-Manager, Domänen-Manager, Scalability-Server und Agent, überwachen. Erstellen Sie einen Alarm oder eine Alarmvorlage, in der Relevanz, Grenzwert und Häufigkeitswerte angegeben werden.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "DSM", "Zustandsüberwachung" und "Alarm-Konfiguration".
2. Konfigurieren Sie die folgenden Entitäten:

   Alarme

   Konfigurieren Sie die Alarmparameter wie Frequenz, Grenzwert und Relevanz der vordefinierten Alarme, und erstellen Sie vorlagen- oder DM-Skript-basierte Alarme.

   Alarm-Vorlagen

   Konfigurieren Sie die Parameter der vordefinierten Alarmvorlagen und erstellen Sie DM-Skript-basierte Vorlagen.

Dadurch wird ein Alarm oder eine Alarmvorlage definiert.

Konfigurieren von Alarmen

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "DSM", "Zustandsüberwachung", "Alarm-Konfiguration" und "Alarme".
2. Wählen Sie "Hinzufügen" aus, um einen Alarm basierend auf einer Vorlage oder einem Skript zu erstellen.
3. Geben Sie die entsprechenden Werte für die folgenden Felder ein:

   Alarmname

   Gibt den Namen des Alarms an.

   Vorlage

   Gibt den Namen der Alarmvorlage an, von der der Alarm abgeleitet wird.

   Hinweis: Wählen Sie eine Vorlage aus der Drop-down-Liste aus, um einen vorlagenbasierten Alarm zu erstellen. Zum Beispiel Asset-Jobs wurden nicht aktualisiert.

   Skript

   Gibt den Skriptnamen für Skript-basierte Alarme an.

   Parameter

   Gibt die für den Alarm geeigneten Parameter an.

   Hinweis: Wenn der Alarm von einer Vorlage abgeleitet wird, werden die Vorlageparameter aus der Vorlage übernommen. Beispiel:
   `GROUPS=ComputerGroups;RequiredPercentage=MINPERCENT;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=TRUE;assetJobNames=%`

   Hinweis: Sie können auch Parameter für Skript-basierte Alarme angeben.

   Meldung

   Definiert die Informationen im Zusammenhang mit dem Alarm, die ausgewertet werden, wenn eine Alarmbedingung erkannt wird. Diese ausgewerteten Informationen werden als Teil des durch den HM-Agenten ausgelösten Alarms weitergegeben. Beispiel:
   `Weniger als $PERCENTAGE der Computer haben die Asset-Jobergebnisse aus der Computergruppe $GROUPS gemeldet`

Relevanz

Konfiguriert die Relevanz des Alarms aus der Drop-down-Liste.

Aktivieren

Gibt den Zustand des Alarms an. Wenn Wahr festgelegt ist, wird der Alarm vom HM-Agenten überwacht, andernfalls ist er von der Überwachung ausgeschlossen.

Erkennungsstufen

Geben die Stufen an, in denen der Alarm erkannt wird. Zum Beispiel EM, DM, SS und Agent.

Hinweis: Wählen Sie bei vordefinierten Alarmen die Stufen aus der unterstützten Liste aus. Wählen Sie bei vorlagenbasierten Alarmen eine Stufe aus der von Vorlagen unterstützten Liste aus.

Frequency

Gibt das Intervall für die Überwachung des Alarms an. Sie können die Frequenz für jede erkannte Stufe in Minuten, Stunden oder Tagen angeben.

Grenzwert

Gibt den Grenzwert an. Dieser Wert gibt an, wie viele Minuten/Stunden/Tage eine Alarmbedingung vorliegen muss, oder wie oft eine Alarmbedingung auftreten muss, bevor ein Alarm ausgelöst wird.

Wenn Sie beispielsweise Der Agent kann nicht mit SS kommunizieren mit einer Frequenz von einer Stunde und einem Grenzwert von sechs Stunden auf der Agentenstufe konfigurieren, prüft der Agent jede Stunde, ob der Agent mit dem Remote-Scalability-Server kommunizieren kann. Bei Fehlern hinsichtlich der Kommunikation für sechs Stunden wird ein Alarm ausgelöst.

4. (Optional) Klicken Sie auf Überprüfen, um die Werte zu überprüfen.
5. Klicken Sie auf Anwenden und anschließend auf OK.

   Der Alarm ist jetzt konfiguriert.

Erstellen DM-Skript-basierter Alarme

Sie können benutzerdefinierte Alarme erstellen, die auf DM-Skripten basieren. Stellen Sie das Skript im Skriptverzeichnis auf dem Agentencomputer bereit, welches sich unter *Konfigurationsrichtlinie, DSM, Zustandsüberwachung, Systemüberwachungs-Agent, ScriptDir* befindet, bevor Sie die für diese Alarme entsprechende Konfiguration anwenden.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "DSM", "Zustandsüberwachung", "Alarm-Konfiguration" und "Alarme".
2. Wählen Sie "Hinzufügen" aus, um einen Alarm anhand eines Skripts zu erstellen, und lassen Sie das Vorlagennamensfeld leer.
3. Geben Sie den Skriptnamen des Domänen-Managers an, der auf den Agentencomputern bereitgestellt wird.
4. Geben Sie die Parameter im Feld "Parameter" an.
5. Fügen Sie im Feld "Meldung" einen Text im Zusammenhang mit dem Alarm hinzu (gegebenenfalls auch Parameter).
6. Legen Sie andere Parameter fest, und wenden Sie sie auf die Agenten für die Überwachung fest.

Beispiel eines Domänen-Manager-Alarms:

Das folgende DM-Skript meldet dem HM-Agenten, ob eine Alarmbedingung vorliegt oder nicht vorliegt, indem "hmAlertOPFormatter" aufgerufen wird. Beispiel:

```
Führen Sie hier die Überprüfung der Alarmbedingung durch.
'...
' Führen Sie unten im DM-Skript hmAlertOPFormatter aus,
' um die Alarm-XML-Ausgabe zu erstellen.
dim ret as integer
ret = Exec("hmAlertOPFormatter.exe alertconditionexist=1 raisealertnow=1
""param1=" + argv(1)  + ",param2=" + argv(2) + """ additionalinfo=this is
some additional text for script with Args", true)
print "hmAlertOPFormatter.exe: " + str(ret)
```

Führen Sie den folgenden Befehl im DM-Skript aus, um eine zu verarbeitende XML-Datei für HM-Agenten zu erstellen, wenn der Aufruf für Überwachungsalarme erfolgt:

Ausführbare Datei "hmAlertOPFormatter"

```
hmAlertOPFormatter.exe alertconditionexist=0|1 [raisealertnow=0|1]
[PARAM1=data1,PARAM2=data2,..,PARAMX=datax] [additional info=Additional Info]
```

`alertconditionexist=0|1`

Verwenden Sie den Wert "0", wenn das DM-Skript keine Alarmbedingung bestimmt hat. Verwenden Sie den Wert "1", wenn das Skript eine Alarmbedingung bestimmt hat.

`raisealertnow=0|1`

(optional) Der Standardwert ist "0". Verwenden Sie den Wert "1", um den Alarm sofort auszulösen.

`PARAM1=data1,PARAM2=data2 .. PARAMX=datax –`

(optional) Diese Schlüssel-Wert-Paare geben die Parameter und ihre Werte in der Alarmmeldung an. Die Schlüssel-Wert-Paare werden mit einem Komma (,) getrennt und die Schlüssel und Werte mit einem Gleichheitszeichen (=).

`additionalinfo=<Additional Info>`

(optional) Dieser Parameter ist der letzte in der Befehlszeile. Der Rest der Befehlszeile nach dem Gleichheitszeichen (=) besteht aus der resultierenden Alarm-XML, die in einem Feld zusammengefügt wird.

Konfigurieren von Alarmvorlagen

Sie können die Alarmvorlagen konfigurieren.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "DSM", "Zustandsüberwachung", "Alarm-Konfiguration" und "Alarm-Vorlagen".
2. Wählen Sie "Hinzufügen" aus, um eine Skript-basierte Alarmvorlage zu erstellen.
3. Geben Sie die entsprechenden Werte für die folgenden Felder ein:

   Alarmname

   Gibt den Vorlagennamen an.

   Vorlage

   Konfiguriert den Namen der Alarmvorlage, von der der Alarm abgeleitet wird. Weitere Informationen finden Sie unter

   Asset-Jobs wurden nicht aktualisiert. (siehe Seite 354)

   Das Asset-Inventar wurde während der Erfassung aus SS nicht aktualisiert. (siehe Seite 355)

Skript

Gibt den Namen des Skripts an. Dieser Name muss dem Namen des Skriptdateinamens entsprechen, der in *ScriptDir* an den HM-Agenten übergeben wurde.

Parameter

Gibt die für das Skript geeigneten Parameter an.

Hinweis: Verwenden Sie durch Semikolon (;) getrennte Namenswertpaare für die Angabe mehrerer Parameter. Verwenden Sie Kommas (,) zum Trennen mehrerer Werte für einen Parameter. Beispiel:
`GROUPS=Group1,Group2;RequiredPercentage=80;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=TRUE;assetJobNames=%`

Meldung

Definiert die Informationen im Zusammenhang mit dem Alarm, die ausgewertet werden, wenn eine Alarmbedingung erkannt wird. Beispiel:
`Weniger als $PERCENTAGE der Computer haben die Asset-Jobergebnisse aus der Computergruppe $GROUPS gemeldet`

Relevanz

Konfiguriert die Relevanz für die Alarmvorlage aus der Drop-down-Liste.

Erkennungsstufen

Geben die Stufen an, in denen der Alarm erkannt wird. Zum Beispiel EM, DM, SS und Agent.

Standardfrequenz

Gibt die Standardfrequenz für die Vorlage an.

Standard-Grenzwert

Gibt den Standard-Grenzwert für die Vorlage an.

4. (Optional) Klicken Sie auf Überprüfen, um die Werte zu überprüfen.
5. Klicken Sie auf Anwenden und anschließend auf OK.

   Die Alarmvorlage ist jetzt konfiguriert.

Vordefinierte Alarmvorlagen

CA ITCM bietet standardmäßig die folgenden Alarmvorlagen.

Asset-Jobs wurden nicht aktualisiert. (siehe Seite 354)

Das Asset-Inventar wurde während der Erfassung aus SS nicht aktualisiert. (siehe Seite 355)

Asset-Jobs wurden nicht aktualisiert.

Diese Vorlage erkennt und löst einen Alarm aus, wenn ein angegebener Prozentsatz an Asset-Jobs für mindestens eine Computergruppe nicht aktualisiert ist.

Parameter

Diese Vorlage unterstützt die folgenden Parameter:

groups=<comma separated list of groups of interest>;

Gibt mindestens einen durch Kommas getrennten Computergruppennamen an.

requiredPercentage=<Required percentage>;

Gibt den erforderlichen Prozentsatz der identifizierten Jobs innerhalb der angegebenen Gruppen an, die erfolgreich sein müssen, um zu vermeiden, dass der Alarm ausgelöst wird.

IncludeLinkedGroupJobs=[TRUE]|[FALSE];

WAHR

Gibt den Wert WAHR an, um Jobs einzubeziehen, die mit Gruppen verknüpft sind. Gleichzeitig werden die einzubeziehenden Jobs für die Überprüfung bestimmt.

FALSCH

Gibt den Wert FALSCH an, um Jobs zu ignorieren, die mit Gruppen verknüpft sind. Gleichzeitig werden die einzubeziehenden Jobs bestimmt.

IncludeLinkedAssetJobs=[TRUE]|[FALSE];

WAHR

Gibt den Wert WAHR an, um Jobs einzubeziehen, die mit Assets verknüpft sind. Gleichzeitig werden die einzubeziehenden Jobs für die Überprüfung bestimmt.

FALSCH

Gibt den Wert FALSCH an, um Jobs zu ignorieren, die mit Assets verknüpft sind. Gleichzeitig werden die einzubeziehenden Jobs bestimmt.

Hinweis: Wenn Sie *IncludeLinkedGroupJobs* oder *IncludeLinkedAssetJobs* in der Parameterliste nicht angeben, verursacht das Standardverhalten, dass die entsprechenden Jobverknüpfungstypen einbezogen werden.

assetJobNames=<comma separated list of job names>

Gibt die erforderlichen Jobnamen für die Evaluierung an. Wenn Sie keine Angabe tätigen, werden alle Asset-Jobs für die angegebene Gruppe bzw. die angegebenen Gruppen für die Evaluierung berücksichtigt.

Hinweis: Sie können mehrere Jobnamen mit durch Kommas getrennte Werte im Parameter "assetJobNames" angeben. Verwenden Sie die folgenden Platzhalterzeichen:

% (Prozentsatz)

Gibt eine Zeichenfolge mit mindestens null Zeichen an. Beispielsweise ist es möglich, mit LIKE %computer%, alle Buchtitel mit dem Wort *computer* zu finden.

_ (Unterstrich)

Gibt ein einzelnes Zeichen an. Beispielsweise ist es möglich, mit *_ean* alle aus vier Buchstaben bestehenden Vornamen zu finden, die auf *ean* enden.

Beispiel für die Parameter für Asset-Jobs wurden nicht aktualisiert:

```
GROUPS=Groups1,Group2;RequiredPercentage=80;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=FALSE;assetJobNames=%
```

Das Asset-Inventar wurde während der Erfassung aus SS nicht aktualisiert.

Diese Vorlage erkennt und löst einen Alarm aus, wenn die Inventaraktualisierung innerhalb eines angegebenen Zeitraums von mindestens einem Scalability-Server oder mindestens einer Scalability-Servergruppe nicht erfolgreich ist.

Parameter

Diese Vorlage unterstützt die folgenden Parameter:

Servers=<comma separated list of scalability server>;

Gibt mindestens einen durch Komma getrennten Server an.

Hinweis: Der Parameter "Server" erfordert den Namen eines im DSM-Explorer aufgeführten Servers, nicht die FQDN.

ServerGroups=<comma separated list of scalability server groups>;

Gibt mindestens eine durch Komma getrennte Servergruppe an.

Hinweis: Der Parameter "Servergruppen" erfordert den Namen einer Gruppe aus "Alle Scalability-Server", "DSM-Explorer", und nicht aus "Alle Computer" und dem Abschnitt "Benutzer".

Hinweis: Wenn Sie die Parameter nicht angeben, werden alle Scalability-Server für die Evaluierung berücksichtigt.

Beispiel für die Parameter für Das Asset-Inventar wurde während der Erfassung aus SS nicht aktualisiert**:**

```
Servers=Server1,Server2;ServerGroups=Group1,Group2
```

Alarm-Collector konfigurieren

Konfigurieren Sie den Alarm-Collector für eine der folgenden Rollen:

Alarme in der MDB beibehalten

Konfiguriert den Alarm-Collector so, dass Alarme in der MDB beibehalten werden.

Alarme in der MDB beibehalten und konfigurierte Aktionen ausführen

Konfiguriert den Collector so, dass Alarme in der MDB beibehalten werden und konfigurierte Aktionen wie das Senden von E-Mails, das Erstellen von SNMP-Traps und das Schreiben in Windows/CCE-Ereignisprotokoll durchgeführt werden.

Alarme beibehalten, Aktionen ausführen und sie weiterleiten

Konfiguriert den Collector so, dass Alarme in der MDB beibehalten, konfigurierte Aktionen durchgeführt und Alarme in einen anderen Alarm-Collector weitergeleitet werden.

Hinweis: Sie können die weiterzuleitenden Alarme basierend auf der Relevanz oder der Erkennungsstufe filtern. Zum Beispiel können Sie festlegen, dass nur Alarme mit hoher und mittlerer Relevanz, die auf dem DM ausgelöst werden, weitergeleitet werden.

Weiterleiten

Konfiguriert den Collector für die Weiterleitung von Alarmen in einen anderen Alarm-Collector.

Hinweis: Der Alarm-Collector wird in einer Cluster-Umgebung nicht unterstützt.

Weitere Informationen zu Alarm-Collector-Rollen finden Sie unter Installieren des Alarm-Collector (siehe Seite 161).

Festlegen von Alarm-Collector-Eigenschaften

Die Konfiguration des Alarm-Collector umfasst das Konfigurieren des Webmoduls und des Alarm-Collector-Prozesses.

Konfiguration des Webmoduls:

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "DSM", "Webservices" und "Zustandsüberwachung".
2. Geben Sie die entsprechenden Werte für die folgenden Optionen ein:

   Ordner zum Hochladen von Alarmen

   Gibt einen Ordner auf dem Rechner mit dem Alarm-Collector an, auf den die Alarm-Info-XML-Dateien hochgeladen werden.

   Standard: *HMAlertUploads.* Dieser Ordner wird relativ zum CA ITCM-Installationsordner angegeben.

   Wenn Sie einen anderen Wert als den Standardwert verwenden, muss das Benutzerkonto, unter dem das Webmodul ausgeführt wird, über Schreibberechtigungen für den Ordner verfügen.

   Hinweis: Ein Netzwerkpfad für den Speicherort des Ordners wird nicht unterstützt.

   Dateien in Alarm-Collector kopieren

   Geben Sie den Wert "1" an, um die hochgeladenen Dateien in den Eingabeordner des Alarm-Collector zu kopieren.

   Standard: 1

   Dateien nach dem Kopieren in Alarm-Collector löschen

   Geben Sie den Wert "1" an, um die Alarm-Info-XML-Dateien nach dem Kopieren in den Eingabeordner des Alarm-Collector zu löschen.

   Standard: 0

Das Webmodul ist jetzt konfiguriert.

Konfiguration des Alarm-Collector-Prozesses:

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Richtlinienname", "DSM", "Zustandsüberwachung" und "Alarm-Collector".
2. Geben Sie die entsprechenden Werte für die folgenden Optionen ein:

   Alarm-Collector-Rolle (Lokal verwaltet)

   Gibt die Rolle an, in der der Alarm-Collector ausgeführt werden muss. Dieser Wert wird anfangs während der Installation festgelegt. Nach der Installation können Sie die Rolle wie folgt in eine andere ändern:

   - Ändern Sie den Rollenparameter in "Zentral verwaltet", legen Sie den Rollenwert fest und wenden Sie ihn auf den Alarm-Collector-Rechner an.
   - Verwenden Sie den CLI-Befehl *ccnfcmda* lokal auf dem Alarm-Collector-Rechner, um diesen Wert festzulegen, und starten Sie den Alarm-Collector-Prozess neu.

   Ordner für Alarminformationen

   Gibt einen Ordner auf dem Rechner mit dem Alarm-Collector an, auf den die Alarm-Info-XML-Dateien hochgeladen werden.

   Standard: AlertCollectorInput. Dieser Ordner wird relativ zum CA ITCM-Installationsordner angegeben.

   Wenn Sie einen anderen Wert als den Standardwert verwenden, muss das Benutzerkonto, unter dem das Webmodul ausgeführt wird, über Schreibberechtigungen für den Ordner verfügen.

   Hinweis: Ein Netzwerkpfad für den Speicherort des Ordners wird nicht unterstützt.

Manager (Lokal verwaltet)

Konfiguriert den Manager, mit dem der Alarm-Collector eine Verbindung herstellen muss. Dieser Wert wird anfangs während der Installation festgelegt. Führen Sie das Verfahren für "Alarm-Collector-Rolle (Lokal verwaltet)" aus, um den Manager nach der Installation zu ändern.

Ausgabeordner

Konfiguriert den Ordner, in dem die Alarm-Info-XML-Dateien nach Bearbeitung durch den Alarm-Collector abgelegt werden.

Standard: AlertCollectorOutput. Dieser Ordner wird relativ zum CA ITCM-Installationsordner angegeben.

Maximales Alarm-Alter bis zur Bereinigung

Gibt an, nach wie vielen Tagen die Alarme bereinigt werden.

Standard: 60 Tage

Alarm: Bereinigungsintervall

Gibt das Intervall an, in dem die Alarme, die älter als das maximale Alarm-Alter bis zur Bereinigung sind, gelöscht werden.

Standard: 10 Tage

Der Alarm-Collector-Prozess ist jetzt eingerichtet.

Konfigurieren von Alarm-Aktionen

Konfigurieren Sie Alarm-Aktionen und wenden Sie diese auf die Alarm-Collector an, die für die folgenden Aktionen konfiguriert sind:

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Richtlinienname", "DSM", "Zustandsüberwachung", "Alarm-Collector", "Alarm-Aktionen" und "Aktionenkonfiguration".

   Das Dialogfeld "Alarm-Aktionen" wird angezeigt.

2. Wählen Sie "Hinzufügen" aus, um eine Aktion für eine der konfigurierten Alarme zu erstellen.

3. Geben Sie die entsprechenden Werte für die folgenden Elemente ein:

   Alarmname

   Legt den Namen des Alarms fest.

   Hinweis: Sie können den Alarm aus der Liste auswählen.

   Mögliche Aktionen

   Geben Sie die folgenden Aktionen nach Bedarf an:

   E-Mail senden

   Sendet die Alarminformationen an die E-Mail-Adresse, die unter *Empfängeradresse* angegeben ist.Wenn keine Adresse angegeben ist, wird die E-Mail an die Empfängeradresse gesendet, die in "SMTP-E-Mail-Konfiguration" global angegeben ist.

   SNMP-Trap erstellen

   Sendet SNMP-Traps an die unter "SNMP-Server" angegebene IP-Adresse. Wenn kein Server angegeben wird, werden Traps an den SNMP-Server gesendet, der unter "Alarm-Aktionen" global angegeben ist.

   In Windows-Ereignisprotokoll schreiben

   Schreibt die Alarminformationen in das Windows-Ereignisprotokoll.

   In CCS-Ereignisprotokoll schreiben

   Schreibt die Alarminformationen in das CCS-Ereignisprotokoll.

   Empfängeradresse

   Konfiguriert die E-Mail-Adresse, an die Sie die Alarminformationen senden. Sie können mehrere, durch Strichpunkt getrennte Adressen angeben.

   SNMP Server

   Konfiguriert den SNMP-Server, an den die SNMP-Traps gesendet werden.

4. Klicken Sie auf Anwenden und anschließend auf OK.

   Aktionen für den Alarm sind jetzt konfiguriert.

Hinweis: Sie können die globalen Einstellungen für SMTP-E-Mail und SNMP-Server über Alarm-Aktionen konfigurieren.

SMTP-E-Mail-Konfiguration

Konfigurieren Sie die SMTP-E-Mail mit den folgenden Angaben:

Absenderadresse

Legt die E-Mail-Adresse fest, die in der Kopfzeile der E-Mail angegeben wird. Beispiel:

Standard: *Systemüberwachungssystem*

Hinweis: Die Absenderadresse darf keine Leerstellen enthalten.

Mail Server

Gibt den DNS-Namen oder die IP-Adresse des SMTP-Mailservers an.

Empfängeradresse

Definiert die E-Mail-Adresse des Empfängers. Sie können mehrere, durch Strichpunkt getrennte Adressen angeben.

Betreff

Gibt den Betreff der E-Mail an.

Standard: *Systemüberwachungsalarm*

Konfigurieren Sie den SNMP-Server mit den folgenden Angaben:

SNMP Server

Konfiguriert den SNMP-Server, an den die SNMP-Traps gesendet werden.

Festlegen der Alarmweiterleitungsdetails

Wenden Sie diese Einstellungen auf die Alarm-Collector an, die in der Weiterleitungsrolle konfiguriert sind.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Richtlinienname", "DSM", "Zustandsüberwachung", "Alarm-Collector", "Alarmweiterleitung".
2. Geben Sie die entsprechenden Werte für die folgenden Elemente ein:

   Alarm-Collector-Adresse

   Gibt den Hostnamen oder die IP-Adresse des Alarm-Collector-Servers an, zu dem die Alarme weitergeleitet werden.

   Alarmweiterleitung: Alarmerkennungsstufe

   Gibt die Stufen an, die bei der Weiterleitung von Alarmen als Filter verwendet werden.

   Standard: DM

   Alarmweiterleitung: Alarmrelevanz

   Gibt die Alarmrelevanz an, die bei der Weiterleitung von Alarmen als Filter verwendet wird.

   Alarmweiterleitung: Ordner für ausstehende Weiterleitungen

   Gibt den Ordner an, in dem die Alarm-Info-XML-Dateien abgelegt werden, die beim ersten Versuch nicht weitergeleitet wurden.

   Alarmweiterleitung: Ordner für abgelehnte Weiterleitungen

   Gibt den Ordner an, in dem die Alarm-Info-XML-Dateien abgelegt werden, die nicht mehr weitergeleitet werden.

   Wiederholungsintervall

   Gibt das Zeitintervall in Minuten an, in dem die Weiterleitung ausstehender Alarme wiederholt wird.

   HTTPS verwenden

   Legt die Verwendung von HTTPS oder einfachem HTTP für die Verbindung mit dem Server fest. Wenn Wahr festgelegt ist, wird https verwendet. Informationen zur entsprechenden Konfiguration, damit der Alarm-Collector eine Verbindung über HTTPS herstellt, finden Sie unter Konfigurieren der Einstellungen für das Hochladen von Alarmen (siehe Seite 366).

Die Alarmweiterleitungsdetails sind jetzt konfiguriert.

Collector-Einstellungen weiterleiten

Konfiguriert die Authentifizierungsdetails, die für die Verbindung mit und die Authentifizierung bei dem Alert-Collector-Server verwendet werden, an den die Alarme weitergeleitet werden.

Weitere Informationen finden Sie unter Konfigurieren der Servereinstellungen des Alarm-Collector (siehe Seite 367).

Einstellungen des Proxy-Servers

Konfiguriert die Details des Proxy-Servers, die verwendet werden, um für die Alarmweiterleitung eine Verbindung mit dem Alarm-Collector-Server herzustellen.

Weitere Informationen finden Sie unter Konfigurieren von Proxyeinstellungen (siehe Seite 368).

Konfigurieren des Systemüberwachungs-Agenten

Ändern Sie die Eigenschaften für den Systemüberwachungs-Agenten.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Richtlinienname", "DSM", "Zustandsüberwachung" und "Systemüberwachungs-Agent".
2. Geben Sie im Dialogfeld "Eigenschaften der Einstellung" geeignete Werte für die folgenden Elemente an:

   Systemüberwachung aktivieren

   Gibt den Status der Systemüberwachung an. Standard: False

   Wahr

   Aktiviert die Systemüberwachung.

   False

   Deaktiviert die Systemüberwachung.

   Skriptverzeichnis

   Gibt den Ordner an, in den benutzerdefinierte Alarmskripte kopiert werden müssen. Standard: scriptdir

   Hinweis: Bei einem absoluten Pfad wird der Pfad nicht angegeben, der Order wird verwendet, der mit dem HM-Ordner unter dem DSM-Installationsverzeichnis in Bezug steht. Netzwerkpfade werden nicht unterstützt.

   Skriptausgabeverzeichnis

   Definiert den Namen des Ordners, in den die Ausgabe von benutzerdefinierten Alarmskripten kopiert werden. Standard: scriptoutputdir

   Hinweis: Bei einem absoluten Pfad wird der Pfad nicht angegeben, der Order wird verwendet, der mit dem HM-Ordner unter dem DSM-Installationsverzeichnis in Bezug steht. Netzwerkpfade werden nicht unterstützt.

   Skript-Zeitlimit

   Definiert die Zeitdauer in Sekunden, die der Systemüberwachungs-Agent wartet, bis die Skriptausführung abgeschlossen ist. Standard: 120 Sekunden

   Hinweis: Wenn die Skriptausführung wegen eines Zeitüberschreitungsfehlers fehlschlägt, erhöhen Sie die Zeit in Sekunden, und versuchen Sie es erneut.

   Maximale Anzahl an Hochladeversuchen

   Legt fest, wie oft versucht wird, Alarminformationen hochzuladen. Standard: 3

   Wiederholungsintervall für Hochladevorgänge

Definiert das Intervall in Sekunden, in dem erneut versucht wird, die Alarminformationen hochzuladen. Standard: 5 Sekunden.

3. Klicken Sie auf "OK".

Der Systemüberwachungs-Agent ist jetzt aktiviert.

Sie müssen auch zusätzliche Parameter für die HM-Ereignisprotokollierung konfigurieren.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM", "Allgemeine Komponenten", "Ereignisprotokoll", "Health Monitoring Events" (Zustandsüberwachungsereignisse).
2. Konfigurieren Sie die folgenden Parameter:

   Ereignisprotokoll-Zielordner

   Definiert den Speicherort relativ zum DSM-Installationsordner für die Ereignisprotokolldateien. Der Ordner muss auf dem Agenten vorhanden sein.

   Standard: HM

   Ereignisprotokoll-Dateiname

   Definiert den für die Protokollierung der Zustandsüberwachungsereignisse zu verwendenden Dateinamen.

   Standard: hmevents_list.xml

Konfigurieren der Einstellungen für das Hochladen von Alarmen

Konfigurieren Sie die Details des Alarm-Collector-Servers, und wenden Sie diese auf den Agenten an, damit der Systemüberwachungs-Agent die erkannten Alarme hochladen kann.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Richtlinienname", "DSM", "Webservices", "Client" und "Zustandsüberwachung".
2. Geben Sie die entsprechenden Werte für die folgenden Optionen ein:

   Alarm-Collector-Adresse

   Gibt den Hostnamen oder die IP-Adresse des Alarm-Collector-Servers an, auf den die Alarme hochgeladen werden.

   Hinweis: Konfigurieren Sie für den HM-Agenten auf dem EM den Alarm-Collector, der auf dem DM installiert ist.

   HTTPS verwenden

   Legt für die Verbindung mit dem Alarm-Collector-Server http oder https fest.

   Standard: "Falsch" zeigt "http" an.

   Wenn der Alarm-Collector für HTTPS konfiguriert ist, führen Sie die folgenden Schritte auf dem Agentencomputer aus:

   - Exportieren Sie das CA-Stammzertifikat im DER-Format vom Webservercomputer (Alarm-Collector).
   - Kopieren Sie das Zertifikat zum Agenten und nehmen Sie einen Import mithilfe des folgenden Befehls vor:

     ```
     cacertutil import -i:<cert-file-path> -it:X509V3 -trust
     ```

Wenn der HM-Agent eine Verbindung mit dem Alarm-Collector über den Proxy herstellen muss und der Alarm-Collector-Server für die Authentifizierung der Client-Anfragen konfiguriert ist, konfigurieren Sie die folgenden Optionen:

Konfigurieren der Servereinstellungen des Alarm-Collector

Konfigurieren Sie die Details der Alarm-Collector-Servereinstellungen wie folgt:

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Richtlinienname", "DSM", "Webservices", "Client", "Zustandsüberwachung" und "Servereinstellungen des Alarm-Collector".
2. Geben Sie die entsprechenden Werte für die folgenden Elemente ein:

   Authentifizierungsmethode

   Legt den Wert fest, der die Authentifizierungsmethode bestimmt.

   Http-Authentifizierungstyp

   Legt den Wert fest, der den Http-Authentifizierungstyp bestimmt.

   Hinweis: Http unterstützt "Standard", "Digest" und "NTLM-Authentifizierung".

   Domäne

   Gibt den Domänennamen des Servers an.

   Kennwort

   Legt das Kennwort zur Authentifizierung beim Proxy fest.

   Anwendername

   Legt den Benutzernamen zur Authentifizierung beim Server fest.

Die Servereinstellungen des Alarm-Collector sind jetzt konfiguriert.

Konfigurieren von Proxyeinstellungen

Konfigurieren Sie die Proxyeinstellungen wie folgt:

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Richtlinienname", "DSM", "Webservices", "Client", "Zustandsüberwachung" und "Einstellungen des Proxy-Servers".
2. Geben Sie die entsprechenden Werte für die folgenden Elemente ein:

   Proxy-Kennwort

   Legt das Kennwort zur Authentifizierung beim Proxy fest.

   Proxy-Benutzer

   Legt den Benutzer für die Authentifizierung beim Server fest.

   Adresse des Proxy-Servers

   Definiert die Adresse des Proxy-Servers.

   Proxy-Server-Port

   Legt den Port fest, den der Proxy bezüglich Verbindungsanfragen prüft.

   Proxy-Typ

   Legt den Wert fest, der den Proxy-Typ bestimmt. Der Wert *Keine* gibt eine direkte HTTP-Verbindung an.

Die Proxyeinstellungen sind jetzt konfiguriert.

Hinweis: Der HM-Agent unterstützt nur HTTP-Proxy. In dieser Version steht der SOCKS-Proxysupport nicht zur Verfügung.

Verwalten und Verfolgen des Status von Alarmen von WAC

Alarm-Anzeige

Wenn ein neuer Alarm ausgelöst wird, wird eine Benachrichtigung im Portlet "Systemstatus" des Domänenknotens im DSM-Explorer angezeigt. Diese Benachrichtigung umfasst einen Hyperlink, der WAC startet und den Benutzer zur Seite "Alarme" weiterleitet, wenn die vereinheitlichte Anmeldung aktiviert ist. Zeigen Sie abgesehen vom Hyperlink die Anzahl der neu ausgelösten Alarme an.

So konfigurieren Sie die vereinheitlichte Anmeldung für WAC:

Gehen Sie wie folgt vor:

1. Navigieren Sie zu Datei "WAC Config.properties" unter "DSM\Web Console\webapps\wac\WEB-INF\classes\com\ca\wac\config\".
2. Legen Sie den Wert von "attemptUnifiedLogin" auf **wahr** fest.
3. Starten Sie Tomcat neu.

   ```
   caf stop tomcat
   ```

   ```
   caf start tomcat
   ```

Die vereinheitlichte Anmeldung für WAC wird jetzt konfiguriert.

Sie können die WAC-Verknüpfung für die Alarm-Anzeige konfigurieren.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Richtlinienname", "DSM", "Zustandsüberwachung", "Alarm-Anzeige" und "WAC".
2. Konfigurieren Sie die Verknüpfung zur Seite der WAC-Alarme.

   Standard: http://localhost/wac?context_launch_class=DSMHMAlert

   Hinweis: Ersetzen Sie *localhost* durch WAC-Computerhostnamen.

Verwalten und Verfolgen des Status von Alarmen von WAC

Verwalten Sie Alarme von WAC, indem Sie Hinweise hinzufügen und den Status auf "Neu", "Weiterverfolgen" oder "Gelöscht" aktualisieren.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Alarme".

   Die Seite "Alarme" wird angezeigt.

2. Wählen Sie einen oder mehrere Alarme und Aktualisieren oder Löschen aus.

   Das entsprechende Dialogfeld wird geöffnet.

   - Ändern Sie zum Aktualisieren den Status des Alarms bzw. der Alarme über die Drop-down-Option:

     Neu

     Gibt den Alarm als "Neu" an.

     Weiterverfolgen

     Gibt den Alarm mit dem Status "Weiterverfolgen" an.

     Gelöscht

     Gibt den Status des Alarms als "Gelöscht" an.

   - Wählen Sie die zu löschenden Alarme aus, und bestätigen Sie den Löschvorgang.

     Hinweis: Um alle Alarme zu löschen, wählen Sie die Option "Alle löschen" aus.

3. Geben Sie unter Hinweise neue nützliche Informationen an, um den Status des Alarms zu verfolgen.

Die Alarme sind jetzt aktualisiert oder gelöscht.

Hinweis: Sie können Alarme nur über die Domain Manager-Ebene verfolgen, aktualisieren und löschen. Alle HM-Alarme im Enterprise-Manager sind schreibgeschützt.

Alarmreplikation

Die Alarmreplikation hilft bei der Replikation von Alarmen.

- Wenn die Aktualisierungen für die Alarme im Domänen-Manager durch die Engine an den Enterprise-Manager repliziert werden, werden neue Alarme nicht als Bestandteil der Replikation erstellt. Die Alarme werden auf dem Enterprise-Manager nur durch die Alarmweiterleitung im Domänen-Manger mit den entsprechenden Filtern erstellt.
- Bevor die Engine einen Alarm an den Enterprise-Manager repliziert, prüft die Engine, ob der Alarm vorhanden ist. Wenn ein Alarm nicht gefunden wird, reproduziert die Engine den Alarm nicht nach oben. Wenn ein Alarm im Domänen-Manager gelöscht wird, wird der entsprechende Alarm auf dem Enterprise-Manager ebenfalls gelöscht.
- Wenn die Verknüpfung eines Domänen-Managers zum Enterprise-Manager aufgehoben wird, steuert der folgende verwaltete Konfigurationsrichtlinienparameter, ob alle Alarme mit "domain_uuid" dieses Domänen-Managers im Enterprise-Manager verbleiben oder gelöscht werden. Bei derartigen Löschvorgängen repliziert die Engine die Alarme nicht erneut vom Domänen-Manager zum Enterprise-Manager. Dieses Verhalten stellt eine Einschränkung dar, wenn der Domänen-Manager erneut mit dem Enterprise-Manager verknüpft wird.

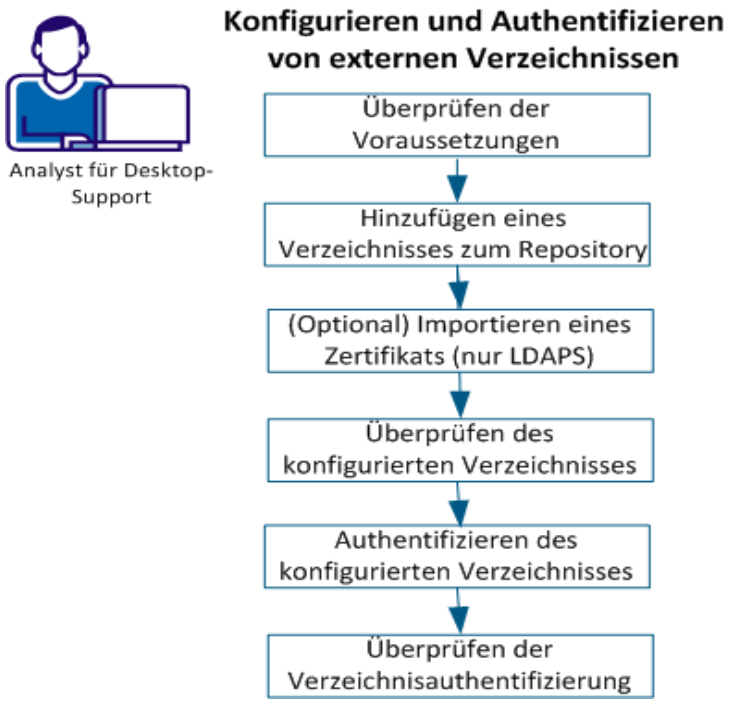
Um den Parameter zu bearbeiten, der die Löschung von Alarmen einer bestimmten Domäne beim Aufheben der Domänenverknüpfung vom Enterprise-Manager steuert, navigieren Sie zu "Systemsteuerung", "Konfiguration", "Konfigurationsrichtlinie", "Standardcomputerrichtlinie", "DSM", "Manager", "Engines", "Replizierte Alarme bei Aufheben der Verknüpfen löschen". Legen Sie zudem beim Aufheben einer Domänen-Manager-Verknüpfung den Wert auf "Wahr" fest, wobei die replizierten Alarme aus dem Domänen-Manager auf dem Enterprise-Manager gelöscht werden.

Kapitel 10: Konfigurieren und Authentifizieren von externen Verzeichnissen

Desktop-Support-Analysten verwenden externe Verzeichnisse für die *Authentifizierung* .Mithilfe der externen Verzeichnisse im DSM-Explorer können Sie die folgenden Tasks durchführen:

- Authentifizieren von Benutzern, einschließlich der Benutzer von Active Directory im systemeigenen Modus.
- Autorisieren von Benutzern durch Zuordnen von Sicherheitsprofilen zu Entitäten im Verzeichnis.
- Definieren von Abfragegruppen mit Zielen, die mit Computern oder Benutzern in einem Container eines Verzeichnisses übereinstimmen.
- Festlegen von Zielen für die Agentenbereitstellung.
- Erstellen von Berichten mithilfe einer Hierarchie aus einem Verzeichnis.

Gehen Sie folgendermaßen vor, um die Authentifizierung mithilfe externer Verzeichnisse durchzuführen:


Konfigurieren und Authentifizieren von externen Verzeichnissen
Analyst für Desktop-Support
Überprüfen der Voraussetzungen
Hinzufügen eines Verzeichnisses zum Repository
(Optional) Importieren eines Zertifikats (nur LDAPS)
Überprüfen des konfigurierten Verzeichnisses
Authentifizieren des konfigurierten Verzeichnisses
Überprüfen der Verzeichnisauthentifizierung

Gehen Sie folgendermaßen vor:

1. Hinzufügen eines Verzeichnisses zum Repository (siehe Seite 375)
2. (Optional) Importieren eines Zertifikats (nur LDAPS) (siehe Seite 380)
3. Überprüfen des konfigurierten Verzeichnisses (siehe Seite 381)
4. Authentifizieren des konfigurierten Verzeichnisses (siehe Seite 385)
5. Überprüfen der Verzeichnisauthentifizierung (siehe Seite 388)

Unterstützte externe Verzeichnisse

CA ITCM unterstützt die folgenden Verzeichnisse:

- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory
- Novell Directory Services (NDS)

Unter Kompatibilitätsmatrix finden Sie eine aktualisierte Liste der unterstützten Verzeichnisintegrationsservices.

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, um die Authentifizierung mithilfe eines externen Verzeichnisses durchzuführen:

- Stellen Sie sicher, dass Sie über die Zugriffsberechtigungen verfügen, um ein externes Verzeichnis zu konfigurieren.
- Sie müssen mit den Verzeichnisintegrationsfunktionen vertraut sein.

Hinzufügen eines Verzeichnisses zum Repository

Um Benutzer durch die Zuordnung von Sicherheitsprofilen zu Entitäten im Verzeichnis zu authentifizieren und zu genehmigen, fügen Sie zunächst das externe Verzeichnis zum Repository hinzu.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Verzeichnisintegration", Verzeichnis hinzufügen", um den Assistenten zum Hinzufügen von Verzeichnissen aufzurufen. Klicken Sie auf "Weiter".

   Die Seite "Einführung/Verzeichnisname" wird angezeigt.

2. Geben Sie unter Verzeichnisname den Verzeichnisnamen an, um das Verzeichnis beim Herstellen einer Verbindung mit Active Directory zu identifizieren.

3. Wählen Sie den Verzeichnistyp anhand einer der Verzeichnistyp-Optionen aus. Folgende Optionen stehen zur Verfügung:

   - Active Directory
   - LDAP
   - NDS

   Standard: Active Directory.

4. Klicken Sie auf "Weiter", um die Seite "Serverdetails" aufzurufen.

Angeben der Verzeichnisserverdetails

Auf der Seite "Serverdetails" des Assistenten können Sie den Namen des Verzeichnisservers angeben, der das hinzuzufügende Verzeichnis enthält, sowie die Nummer des Ports für die Verbindung.

Hinweis: Für externe Verzeichnisse, die Secure Sockets Layer (SSL) verwenden, muss das vom LDAP-Server (Lightweight Directory Access Protocol) verwendete Zertifikat gültig und über die Kette der Microsoft Windows-Zertifizierungsstellen zertifizierbar sein. In früheren Windows-Version hatte der LDAP-Entwickler die Möglichkeit, Zertifikate zu verifizieren, in Windows 2003 SSL wird dies jedoch erzwungen.

Gehen Sie wie folgt vor:

1. Geben Sie den Namen des Servers, der das Verzeichnis unterstützt, im Feld "Servername" ein.
2. Geben Sie im Feld "Port" die Port-Nummer für den Verzeichnisdienst an.

   Der Verzeichnis-Client versucht immer, mit Hilfe des hier angegebenen Ports eine sichere verschlüsselte Verbindung zum Verzeichnis herzustellen. Einige Verzeichnisse unterstützen Port 389 für sichere und nicht sichere Verbindungen. Einige Verzeichnisse unterstützen auch Port 636 ausschließlich für sichere Verbindungen. Ihr Verzeichnisadministrator kann Ihnen sagen, welchen Port Sie verwenden müssen.

   Für den angegebenen Port wird ein sicherer Kanal verwendet, falls vorhanden. Wenn über den angegebenen Port eine nicht sichere Kommunikation möglich ist, wird diese verwendet. (Wenn eine nicht sichere Kommunikation unzulässig ist, wird der Verzeichnisimport nach dem Klicken auf "Fertig stellen" mit einer entsprechenden Fehlermeldung abgelehnt.)

   Hinweis: Allgemeine Konfigurationsrichtlinien für Verzeichnisse, insbesondere die Richtlinie "Einfache LDAP-Authentifizierung aktivieren", können Einfluss darauf haben, ob die Authentifizierung über einen nicht sicheren Kommunikationskanal stattfinden kann.
3. Klicken Sie auf "Weiter", um die Seite "Verzeichnisbindung" aufzurufen.

Hinweis: Wenn Sie ein LDAP-Verzeichnis hinzugefügt haben und anschließend der angegebene Zugangsport geändert wird, wird die *ursprüngliche* Sicherheitsautorität nicht ordnungsgemäß entfernt, und die Liste mit den Sicherheitsautoritäten kann eine ungültige Sicherheitsautorität enthalten. Dies wirkt sich zwar nicht auf die Funktionen von CA ITCM aus, jedoch wird die ursprüngliche Sicherheitsautorität in Sicherheitsdialogfeldern in der entsprechenden Liste als gültig angezeigt. Zum Entfernen der irrelevanten Sicherheitsautorität benötigen Sie ein entsprechendes Tool vom Technischen Support. Wenden Sie sich an Ihren Support-Berater, und fragen Sie nach dem Hilfsprogramm *cfspsetpass*.

Angeben von Informationen zur Verzeichnisbindung

Auf der Seite "Verzeichnisbindung" des Assistenten können Sie angeben, ob der Zugriff auf das Verzeichnis anonym oder mit Benutzeranmeldeinformationen erfolgen soll.

Gehen Sie wie folgt vor:

1. (Optional) Wählen Sie die Option "Anonyme Bindung verwenden". Standardmäßig ist diese Option nicht ausgewählt ("Falsch").

   Hinweis: Wenn diese Option aktiviert ist, haben Sie möglicherweise nur eingeschränkten oder gar keinen Zugriff auf das Verzeichnis.

2. Geben Sie den Benutzernamen und das Kennwort in den entsprechenden Feldern ein.

3. (Optional) Wählen Sie die Option "Sicheres Protokoll (LDAPS) verwenden". Wenn Sie diese Option auswählen, wird das sichere LDAPS-Protokoll statt LDAP verwendet. Stellen Sie jedoch sicher, dass LDAPS von dem Verzeichnis unterstützt wird, das Sie konfigurieren.

   Hinweis: Das Feld wird nur angezeigt, wenn Sie ein Active Directory- oder LDAP-Verzeichnis konfigurieren.

4. Klicken Sie auf "Weiter", um die Seite "Basisverzeichnisknoten" aufzurufen.

Angeben von Details zum Basisverzeichnisknoten

Auf der Seite "Basisverzeichnisknoten" des Assistenten können Sie einen Root-Knoten als Startpunkt zum Durchsuchen des Verzeichnisses angeben.

Gehen Sie wie folgt vor:

1. Geben Sie im Feld "Basisverzeichnisknoten" den eindeutigen Namen (Distinguished Name - DN) des Root-Objektes zum Durchsuchen des aktuellen Verzeichnisses ein.

   Hinweis: Versuchen Sie, einen Basis-DN zu verwenden, der in der Verzeichnishierarchie möglichst weit unten ist, damit die Suchvorgänge effizienter gestaltet sind. Welcher Wert am besten geeignet ist, erfahren Sie von Ihrem Verzeichnisadministrator.

2. Klicken Sie auf "Weiter", um die Seite "Schemazuordnung wählen" aufzurufen.

Auswählen der Schemazuordnungsattribute

Auf der Seite "Schemazuordnung wählen" des Assistenten können Sie die Schemazuordnung festlegen, die für Ihr Verzeichnis verwendet werden soll. Sie können entweder eine vordefinierte allgemeine Schemazuordnung aus der Liste auswählen oder eine eigene definieren.

Gehen Sie wie folgt vor:

1. (Optional) Wählen Sie die Option "Neue Zuordnung definieren", wenn Sie Ihre eigene Schemazuordnung verwenden möchten.

   Diese Option ermöglicht Ihnen die Definition einer Zuordnung der mit Datenobjekten wie Benutzern, Computern und Gruppen verknüpften Attributnamen, die in Ihrem externen Verzeichnis verwendet werden, zu den Attributnamen, die von den entsprechenden DSM-Objekten verwendet werden.

2. Wählen Sie eine vordefinierte Schemazuordnung anhand einer der Schemazuordnungsoptionen aus. Gültige Optionen sind "Active Directory", "eTrust Directory" und "NDS Directory".

   Standard: Active Directory

3. Klicken Sie auf "Weiter", um die Seite "Schemazuordnung verfeinern/festlegen" aufzurufen.

Verfeinern/Festlegen von Schemazuordnungsdetails

Auf der Seite "Schemazuordnung verfeinern/festlegen" des Assistenten können Sie eine neue Schemazuordnung festlegen oder das angegebene Schema verfeinern. Das Schema des Verzeichnisses legt die Namen und Typen der Attribute fest. Die Schemazuordnung überträgt die Attribute eines Verzeichnisobjekts oder Eigenschaften, die in dem Schema des Verzeichnisses definiert sind, in ein allgemeines Schema, das von anderen DSM-basierten Anwendungen verwendet wird.

Hinweis: Für die gängigsten Schemen steht eine Reihe vordefinierter Schemazuordnungen zur Verfügung, einschließlich hartcodierter Zuordnungen für WinNT- und UnixL-Provider.

Gehen Sie wie folgt vor:

1. Wenn Sie ein neues Schema erstellen, geben Sie im Feld "Schemaname" einen eindeutigen Namen für das Schema ein. Andernfalls zeigt dieses Feld den ausgewählten Namen des vorhandenen Schemas an.

   Es wird die entsprechende Zuordnungstabelle geöffnet, in der die Namen und Typen der Attribute im Schema des angegebenen Verzeichnisses aufgeführt sind.

2. (Optional) Klicken Sie zum Ändern des Standardwerts eines DSM-Attributs auf das entsprechende Attribut in der Zuordnungstabelle.

   Das Dialogfeld "Attributzuordnung" wird angezeigt.

3. (Optional) Ändern Sie den Wert von einem oder mehreren DSM-Attributen, und klicken Sie auf "OK".

   Das Dialogfeld "Attributzuordnung" wird geschlossen, und es wird wieder die Assistentenseite angezeigt.

4. Klicken Sie auf "Weiter", um die Seite "Fertig stellen" aufzurufen.

Weitere Informationen zu Schemen finden Sie unter Schemazuordnung (siehe Seite 391).

Überprüfen der Konfigurationsoptionen und Hinzufügen des Verzeichnisses

Diese Seite "Fertig stellen" des Assistenten enthält eine Zusammenfassung der Konfigurationseinstellungen und Optionen, die Sie für das Verzeichnis ausgewählt haben. Klicken Sie auf "Fertig stellen", um den Vorgang zum Hinzufügen des angegebenen Verzeichnisses zum Repository abzuschließen, oder klicken Sie auf "Zurück", um Einstellungen und Optionen zu ändern, und klicken Sie dann auf "Fertig stellen".

Das externe Verzeichnis ist jetzt konfiguriert.

(Optional) Importieren eines Zertifikats (nur LDAPS)

Wenn Sie LDAPS verwenden, um den Zugriff auf ein bestimmtes LDAP- oder OpenLDAP-Verzeichnis zu sichern, muss der Windows-Server in der Lage sein, das Zertifikat des LDAPS-Servers als vertrauenswürdig einzustufen. Wenn das Zertifikat nicht von einer vertrauenswürdigen Zertifizierungsstelle stammt, müssen Sie das Zertifikat manuell in den Zertifikatspeicher importieren, um den Konfigurationsprozess für das neue Verzeichnis abzuschließen.

Hinweis: Ausführliche Informationen zu den Assistenten und Dialogfeldern in der folgenden Prozedur finden Sie in der Microsoft-Dokumentation zu x.509-Zertifikaten.

Gehen Sie wie folgt vor:

1. Suchen Sie die Datei "...\CA\DSM\bin\itrm_dsm_r11_root.der", und doppelklicken Sie darauf.

   Das Dialogfeld "Zertifikat importieren" wird angezeigt.

2. Klicken Sie auf "Zertifikat installieren".

   Der Assistent für den Zertifikatsimport wird angezeigt.

3. Klicken Sie auf "Weiter".

   Die Assistentenseite "Zertifikatspeicher" wird angezeigt.

4. Wählen Sie die Option "Alle Zertifikate in folgendem Speicher ablegen".

5. Klicken Sie auf Durchsuchen.

   Das Dialogfeld "Zertifikatspeicher auswählen" wird angezeigt.

6. Wählen Sie die Option "Physikalischen Speicher anzeigen".

7. Führen Sie *einen* der folgenden Schritte aus:

   - Wenn das Zertifikat selbstsigniert ist, erweitern Sie den Ordner "Trusted Root Certification Authorities", und wählen Sie "Lokaler Computer".
   - Wenn das Zertifikat *nicht* selbstsigniert ist, erweitern Sie den Ordner "Third-Party Root Certification Authorities", und wählen Sie "Lokaler Computer".

   Wichtig! Dieser Schritt ist wichtig. Das Zertifikat muss zum physischen Speicher hinzugefügt werden, da sonst der Speicher des aktuellen Benutzers verwendet wird und das Zertifikat nicht dem von CA ITCM verwendeten lokalen Systemkonto zur Verfügung steht.

8. Klicken Sie auf "OK".

   Das Dialogfeld wird geschlossen, und es wird wieder die Assistentenseite angezeigt.

9. Klicken Sie auf "Weiter" und "Fertig stellen".

   Die Meldung Der Import war erfolgreich wird angezeigt.

10. Klicken Sie auf "OK".

Das angegebene Zertifikat wurde zum Zertifikatspeicher hinzugefügt.

Hinweis: Sie können denselben Vorgang auch mit Hilfe des Befehls "encUtilCmd certimport" ausführen.

Überprüfen des konfigurierten Verzeichnisses

Nachdem Sie das Verzeichnis hinzugefügt und konfiguriert haben, können Sie überprüfen, ob das konfigurierte Verzeichnis im DSM-Explorer hinzugefügt wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Systemsteuerung", "Verzeichnisintegration" und zum Knoten "Configured Directories" (Konfigurierte Verzeichnisse).

   Der Name und die Beschreibung aller konfigurierten *externen Verzeichnisse* in der aktuellen Domäne werden angezeigt. In der Spalte "Beschreibung" wird eine LDAP-URL für alle konfigurierten Active Directory-Verzeichnisse angezeigt, sofern vorhanden.

Das externe Verzeichnis ist jetzt konfiguriert.

(Optional) Aktualisieren des Verzeichnisses

Sie können auch die Verzeichniseigenschaften aktualisieren.

1. (Optional) Aktualisieren Sie ein konfiguriertes Verzeichnis mithilfe der Eigenschaften eines konfigurierten Verzeichnisses.

   Das Dialogfeld "Update Directory" (Verzeichnis aktualisieren) wird mit den folgenden Registerkarten angezeigt.

   - Einstellungen (siehe Seite 382)
   - Sicherheit
   - Schema (siehe Seite 384)

Verzeichnis aktualisieren: Registerkarte "Einstellungen"

Die Registerkarte "Einstellungen" enthält die Hauptkonfigurationsoptionen für Verzeichnisse.

Diese Registerkarte enthält die folgenden Felder:

Verzeichnisname

Gibt das Verzeichnis, den Verzeichnisserver oder den Namen der NDS-Baumstruktur folgendermaßen an:

- Gibt den Namen an, der zur Identifizierung bei einer Verbindungsherstellung zu Active Directory verwendet wird. Dabei muss es sich um einen Namen handeln, den das Verzeichnis selbst in einen Verzeichnisserver auflösen kann.
- Gibt den Namen des Verzeichnisservers bei der Verbindungsherstellung zu einem eigenständigen Verzeichnis (d. h. kein verteiltes Verzeichnis wie Active Directory) mit LDAP an. Bei dem Namen muss es sich um den vollständigen DNS-Namen des Servers handeln, der für den Zugriff auf und die Autorisierung beim Verzeichnis verwendet wird.
- Gibt den Namen der NDS-Baumstruktur bei der Herstellung einer Verbindung zu Novell NDS an.

Beispiel: Eine Active Directory-Domäne HQDirectory.com wird auf dem Computer FAKE_MACHINE gehostet. Wenn Sie dieses Verzeichnis für die Integration konfigurieren, könnten Sie in diesem Feld "HQDirectory.com" angeben, da Active Directory HQDirectory.com in FAKE_MACHINE auflösen kann.

Verzeichnistyp

Gibt den Verzeichnistyp an. Gültige Optionen sind "Active Directory", "LDAP" und "NDS". Standardmäßig ist der Verzeichnistyp ausgewählt, der beim Hinzufügen des Verzeichnisses angegeben war.

Verzeichnisserver

Gibt den Namen des Servers an, der das Verzeichnis unterstützt.

Port

Geben Sie die Portnummer für den Directory Service an. Der Verzeichnis-Client versucht immer, mit Hilfe des hier angegebenen Ports eine sichere verschlüsselte Verbindung zum Verzeichnis herzustellen. Einige Verzeichnisse unterstützen Port 389 für sichere und nicht sichere Verbindungen. Einige Verzeichnisse unterstützen auch Port 636 ausschließlich für sichere Verbindungen. Ihr Verzeichnisadministrator kann Ihnen sagen, welchen Port Sie verwenden müssen.

Für den angegebenen Port wird ein sicherer Kanal verwendet, falls vorhanden. Wenn über den angegebenen Port eine nicht sichere Kommunikation möglich ist, wird diese verwendet. (Wenn eine nicht sichere Kommunikation unzulässig ist, wird der Verzeichnisimport nach dem Klicken auf "Fertig stellen" mit einer entsprechenden Fehlermeldung abgelehnt.)

Hinweis: Allgemeine Konfigurationsrichtlinien für Verzeichnisse, insbesondere die Richtlinie "Einfache LDAP-Authentifizierung aktivieren", können Einfluss darauf haben, ob die Authentifizierung über einen nicht sicheren Kommunikationskanal stattfinden kann. Weitere Informationen finden Sie im Abschnitt "Konfigurationsrichtlinie" in der *DSM-Explorer-Hilfe*.

Standard: 389 (für LDAP-Verzeichnisse)

Basis-DN

Gibt den Distinguished Name (DN) des Stammobjekts für das Durchsuchen des aktuellen Verzeichnisses an. Fragen Sie Ihren Verzeichnisadministrator, welcher Wert am besten geeignet ist.

Hinweis: Da über diesen Basisknoten unter Umständen viele Suchvorgänge im Verzeichnis durchgeführt werden, sollten Sie sich im Vorfeld Gedanken über die Effizienz und Genauigkeit der durchzuführenden Suchvorgänge machen. Versuchen Sie einen Basis-DN zu verwenden, der in der Verzeichnishierarchie möglichst weit unten ist, da auf diese Weise sichergestellt wird, dass die Suchvorgänge effizienter sind.

Informationen

Zeigt Tipps zur Auswahl von Optionen oder zur Eingabe von Daten in Felder bzw. Dialogfelder an.

Verzeichnis aktualisieren: Registerkarte "Sicherheit"

Die Registerkarte "Sicherheit" umfasst Sicherheitsoptionen für die Verbindung mit dem Verzeichnis.

Diese Registerkarte enthält die folgenden Felder:

Anonymes Binding

Gibt an, ob anonymes Binding verwendet werden sollte. Standardmäßig ist der Wert ausgewählt, der beim Hinzufügen des Verzeichnisses angegeben war.

Anwender

Gibt den Benutzernamen an, wenn anonymes Binding nicht ausgewählt ist.

Kennwort

Gibt das Kennwort für den angegebenen Benutzer an, wenn anonymes Binding nicht ausgewählt ist.

Informationen

Zeigt Tipps zur Auswahl von Optionen oder zur Eingabe von Daten in Felder bzw. Dialogfelder an.

Verzeichnis aktualisieren: Registerkarte "Schema"

Die Registerkarte "Schema" umfasst die Konfigurationsoptionen zum Zuordnen von Verzeichnisattributen zum CA ITCM-Schema.

Diese Registerkarte enthält die folgenden Felder:

Schema

Zeigt das zu verwendende Schema an. Für die gängigsten Schemen steht eine Reihe vordefinierter Schemazuordnungen zur Verfügung, einschließlich hartcodierter Zuordnungen für WinNT- und UnixL-Provider. Wählen Sie einen Wert aus der Dropdownliste aus.

Informationen

Zeigt Tipps zur Auswahl von Optionen oder zur Eingabe von Daten in Felder bzw. Dialogfelder an.

Authentifizieren mithilfe des konfigurierten Verzeichnisses

Die Authentifizierung identifiziert Mitglieder einer Trusted Computing Base auf Grundlage der angegebenen Anmeldeinformationen. Fügen Sie die externen Verzeichnisse als Sicherheitsautorität für DSM-Autorisierungsvorgänge hinzu. CA ITCM authentifiziert ein Sicherheitsobjekt für das externe Verzeichnis und verwendet die authentifizierte Identität oder Gruppenmitgliedschaften für folgende Autorisierungsaufrufe.

Wenn beispielsweise ein Linux-DSM-Manager Active Directory-Benutzer unter Verwendung von LDAP authentifizieren soll, stellen Sie sicher, dass Active Directory entsprechend der maximal verfügbaren Sicherheit konfiguriert ist. Verwenden Sie die Zertifizierungsdienste für das Verzeichnis, und stellen Sie sicher, dass die Linux-Installation die Zertifizierungskette des jeweiligen Verzeichniszertifikats als vertrauenswürdig einstuft.

Hinzufügen von Sicherheitsprofilen

Wenn Sie ein Sicherheitsprofil erstellen, wird ein neues Sicherheitsprofil einem Benutzerkonto oder einer Gruppe zugeordnet, die von den aktuellen Sicherheitsprovidern bereitgestellt werden. Sie können die Benutzer oder Gruppen auswählen, die auf das System zugreifen können, und sie einem Sicherheitsprofil hinzufügen.

Gehen Sie wie folgt vor:

1. Wählen Sie im Menü "Sicherheit" die Option "Sicherheitsprofile" aus.

   Das Dialogfeld "Sicherheitsprofile" wird angezeigt.

   Hinweis: Zum Öffnen dieses Dialogfelds müssen Sie über ausreichende Zugriffsrechte verfügen, anderenfalls wird eine Fehlermeldung angezeigt. Administratoren haben standardmäßig diese Zugriffsrechte.

2. Klicken Sie auf "Hinzufügen".

   Das Dialogfeld "Sicherheitsprofile hinzufügen" wird angezeigt.

3. Wählen Sie in der Baumstruktur "Verfügbare Verzeichnisse" die Sicherheitsautorität aus, suchen Sie nach dem erforderlichen Sicherheitsprinzipal, und klicken Sie auf diesen.

   In den Feldern "Container-ID" und "Namen" werden jeweils die ausgewählte Sicherheitsautorität und der Sicherheitsprinzipal angezeigt.

4. Doppelklicken Sie in der Struktur auf einen Prinzipal, oder klicken Sie auf "Zu Liste hinzufügen".

   Die Sicherheitsprinzipale im Feld "Namen" werden der Liste der Sicherheitsprofile hinzugefügt.

   Um weitere Profile hinzuzufügen, wiederholen Sie die letzten beiden Schritte im Dialogfeld "Sicherheitsprofile hinzufügen".

5. Klicken Sie auf "OK".

   Das ausgewählte Benutzerkonto oder die Gruppe wird dem Sicherheitsprofil zugeordnet und das Dialogfeld "Klassenberechtigungen" angezeigt.

   Hinweis: Wenn Sie mehr als ein Sicherheitsprinzipal hinzugefügt haben, wird das Dialogfeld "Klassenberechtigungen" nicht angezeigt. Sie müssen im Dialogfeld "Sicherheitsprofile" das Profil auswählen und auf "Klassenberechtigungen" klicken.

6. Wählen Sie im Dialogfeld "Klassenberechtigungen" die Objektklasse aus, der Sie die Rechte zuweisen möchten.

   Hinweis: Sie können mehrere Objektklassen auswählen und für alle die Klassenberechtigungen angeben. Um eine fortlaufende Auswahl zu treffen, drücken Sie die UMSCHALT-Taste und klicken auf die Objekte. Um eine zufällige Auswahl zu treffen, drücken Sie die STRG-Taste und klicken dann auf die Objekte.

7. Wählen Sie die Berechtigung in der Dropdown-Liste "Klassenzugriff" aus, und klicken Sie auf "OK".

   Die entsprechenden Berechtigungen werden dem neuen Sicherheitsprofil zugewiesen.

Das Dialogfeld "Sicherheitsprofile hinzufügen" wird mit einer Liste der verfügbaren Sicherheitsautoritäten angezeigt: Windows NT-Domänen, UNIX-Authentifizierungsziele, externe Verzeichnisse, z. B. NDS und LDAP, und das Untersystem des X.509-Zertifikats.

Der Manager speichert die Liste der verfügbaren Sicherheitsautoritäten. In einer Windows NT-Domänenumgebung berechnet der Manager-Knoten automatisch alle verfügbaren expliziten Vertrauensverhältnisse für Domänen. Sie können die Liste der verfügbaren Sicherheitsautoritäten über das Dialogfeld "Sicherheitsprofile hinzufügen" anzeigen.

In einigen Fällen ist es sinnvoll, beim Erstellen von Sicherheitsprofilen eine implizit vertrauenswürdige Domäne zu verwenden, also eine Domäne, die nicht in der Ergebnisliste der Berechnung enthalten ist.

Im Dialogfeld "Sicherheitsprofile" können Sie Autoritäten hinzufügen und entfernen, jedoch nur innerhalb des Namespace von Windows NT (winnt).

- Um eine implizit vertrauenswürdige Domäne hinzuzufügen, klicken Sie auf "Hinzufügen" und geben im daraufhin angezeigten Dialogfeld den Namen der Domäne ein.
- Um eine implizit vertrauenswürdige Domäne zu entfernen, markieren Sie die entsprechende Domäne, und klicken Sie auf "Entfernen".

Hinweis: Die Einstufung als vertrauenswürdig wird vom Betriebssystem durchgesetzt. Wenn nicht ohnehin ein Vertrauensverhältnis zwischen einer Domäne und dem Betriebssystem besteht, können Sie diese Domäne nicht hinzufügen, um ein Vertrauensverhältnis zwischen der Domäne und dem Manager zu schaffen.

Vordefinierte Zugriffstypen

Im folgenden Beispiel werden die Auswirkungen der verschiedenen Zugriffsrechte in der Objektklasse "Computer" dargestellt:

Klassenzugriff	Entsprechende Berechtigung
Ansicht	Zeigt alle Computer im Ordner "Alle Computer" an.
Gelesen	Hierüber können Sie die Eigenschaften der Computer anzeigen.
Verwalten	Hierüber können Sie auf einem Computer ein Softwarepaket bereitstellen oder einen Job ausführen.
Ändern	Hierüber können Sie einen Computer hinzufügen oder einen Computer löschen.
Vollzugriff	Hierüber erhalten Sie vollständige Kontrolle über die Computer.

Überprüfen der Verzeichnisauthentifizierung

Um eine erfolgreiche Verzeichnisintegration sicherzustellen, überprüfen Sie die Verzeichnisauthentifizierung, indem Sie sich bei CA ITCM anmelden.

Gehen Sie wie folgt vor: im DSM-Explorer

1. Geben Sie den Benutzernamen und das Kennwort an.

   Definiert den Benutzernamen für die Anmeldung.

   Standard: DN-Format.

   Wichtig! Wenn Sie UID- oder SN-Formate für die Authentifizierung verwenden möchten, konfigurieren Sie den Wert der Konfigurationsrichtlinie entsprechend. Weitere Informationen finden Sie unter Ändern der Richtlinie zur Verwendung eines anderen Formats für den Benutzernamen (siehe Seite 390).

2. Wählen Sie die Sicherheitsautorität aus der folgenden Liste aus:

   Sicherheitsprovider

   Gibt den Sicherheitsprovider an. Da CA ITCM die externen Verzeichnisse, das Benutzerkonto des Betriebssystems sowie Gruppen zum Erteilen von Zugriffsrechten verwendet, fungiert das Betriebssystem als Sicherheitsprovider. Wählen Sie den zutreffenden Sicherheitsprovider aus; die entsprechende Windows-Domäne oder das entsprechende Verzeichnis wird angezeigt.

   Windows-Domäne (Windows) / Verzeichnis (ldap)

   Wählen Sie die Domäne oder den Computer aus, in der/dem Sie über das Benutzerkonto verfügen. Das konfigurierte Verzeichnis, das Zugriff auf CA ITCM hat, wird in der Drop-down-Liste angezeigt.

3. Klicken Sie auf "Anmelden".

   Führt die Anmeldung beim System durch, sofern die Anmeldeinformationen korrekt sind.

Gehen Sie wie folgt vor: für Webkonsolen-Zugriff

1. Wählen Sie den Managernamen aus der Drop-down-Liste der Webkonsole aus.
2. Geben Sie den Benutzernamen und das Kennwort an.

   Definiert den Benutzernamen für die Anmeldung. Sie können das DN-Format verwenden.

   Wichtig! Wenn Sie das UID- oder SN-Format für die Authentifizierung verwenden möchten, konfigurieren Sie den Wert der Konfigurationsrichtlinie entsprechend. Weitere Informationen finden Sie unter Ändern der Richtlinie zur Verwendung eines anderen Formats für den Benutzernamen (siehe Seite 390).
3. Wählen Sie die Sicherheitsautorität aus der folgenden Liste aus:

   Sicherheitsprovider

   Gibt den Sicherheitsprovider an. Da CA ITCM die externen Verzeichnisse, das Benutzerkonto des Betriebssystems sowie Gruppen zum Erteilen von Zugriffsrechten verwendet, fungiert das Betriebssystem als Sicherheitsprovider. Wählen Sie den zutreffenden Sicherheitsprovider aus; die entsprechende Windows-Domäne oder das entsprechende Verzeichnis wird angezeigt.

   Windows-Domäne (Windows) / Verzeichnis (ldap)

   Wählen Sie die Domäne oder den Computer aus, in der/dem Sie über das Benutzerkonto verfügen. Das konfigurierte Verzeichnis, das Zugriff auf CA ITCM hat, wird in der Drop-down-Liste angezeigt.
4. Klicken Sie auf "Anmelden".

   Führt die Anmeldung beim System durch, sofern die Anmeldeinformationen korrekt sind.

Hinweis: Der Administrator auf dem Domänen-Manager authentifiziert den Benutzer mit Zugriffsrechten zum konfigurierten Verzeichnis.

Ändern der Richtlinie zur Verwendung eines anderen Formats für den Benutzernamen

Konfigurieren Sie den Wert der Konfigurationsrichtlinie nur, wenn Sie nicht das DN-Format für die Authentifizierung verwenden. Im Dialogfeld "Eigenschaften von Einstellung" können Sie Konfigurationsrichtlinien ändern, um sie Ihren Anforderungen und Ihrer Umgebung anzupassen.

Hinweis: Vor dem Ändern einer Richtlinie muss die Versiegelung aufgehoben werden.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Konfiguration", "Konfigurationsrichtlinie", "Default Computer Policy" (Standardcomputerrichtlinie), "DSM", "Gemeinsame Komponenten", "Sicherheit", "Provider", "Komponenten", "LDAP".
2. Klicken Sie im Fensterbereich mit der rechten Maustaste auf Oracle ldap: Shortname Type (Oracle LDAP: Typ des Kurznamen), und wählen Sie im Kontextmenü Eigenschaften von Einstellung aus. Klicken Sie alternativ im Portlet "Tasks" auf "Eigenschaften von Einstellung".

   Das Dialogfeld "Eigenschaften von Einstellung" wird geöffnet.
3. Wählen Sie im Feld "Wert" entsprechend Ihrer Anforderungen *einen* der folgenden Werte aus:

   sn

   Gibt den Kurznamen für Oracle LDAP an.

   uid

   Gibt die eindeutige ID für Oracle LDAP an.
4. Klicken Sie auf "OK".

   Der neue Wert gibt an, ob der für die Authentifizierung bereitgestellte Benutzername "sn" oder "uid" ist.

Hinweis: Der *sn* muss für ein Active Directory-basiertes LDAP eindeutig sein.

Schemazuordnungsattribute

Eine *Schemazuordnung* ist eine Zuordnung der mit Datenobjekten wie Benutzern, Computern und Gruppen verknüpften Attributnamen, die in Ihrem externen Verzeichnis verwendet werden, zu den Attributnamen, die von den entsprechenden DSM-Objekten verwendet werden. Der feste Satz und der Standardsatz der DSM-Attributnamen werden zur Abfrage von Verzeichnissen und zur Formulierung komplexer Abfragen und Berichte verwendet.

In CA ITCM stehen drei vordefinierte allgemeine Schemazuordnungen zur Verfügung. Sie haben auch die Möglichkeit, Ihr eigenes benutzerdefiniertes Schema auf der Basis des vordefinierten Schemasatzes zu erstellen.

DSM-Attributnamen

In der nachfolgenden Tabelle finden Sie die Standardattributnamen mit jeweils einer kurzen Beschreibung, die von DSM-basierten Anwendungen für die Abfrage von Verzeichnissen verwendet werden:

Attributname	Beschreibung
objectClass	Klasse der Objekte
dc	Domänen-Controller
o	Organisation
ou	Organisationseinheit
c	Country
l	Standort
userDn	Definierter Name (Distinguished Name) des Benutzers
userCn	Allgemeiner Name (Common Name) des Benutzers
userSn	Nachname des Benutzers
givenName	Vorname des Benutzers
displayName	Anzeigename
userName	Benutzername:
userID	Benutzer-ID
userPassword	Benutzerkennwort
memberOf	Namen/definierte Namen der Gruppen, zu denen ein Benutzer gehört
directReports	Namen/definierte Namen der Personen, die diesem Benutzer unterstellt sind

Attributname	Beschreibung
streetAddress	Straße
postalCode	Postleitzahl
company	Unternehmen
Abteilung	Abteilung
email	E-Mail-Adresse
telephoneNumber	Telefonnummer
jobTitle	Berufsbezeichnung
userDescription	Beschreibung des Benutzers
assetDn	Definierter Name (Distinguished Name) des Computers
assetCn	Allgemeiner Name (Common Name) des Computers
assetName	Name des Computers
dnsHostName	DNS-Hostname
operatingSystem	Betriebssystem
operatingSystemServicePack	Betriebssystem-Service Pack
operatingSystemVersion	Betriebssystemversion
assetDescription	Beschreibung des Computers
groupDn	Definierter Name (Distinguished Name) der Gruppe
groupCn	Allgemeiner Name (Common Name) der Gruppe
groupName	Name der Gruppe
groupMembers	Namen/definierte Namen der Benutzer, die Mitglieder der Gruppe sind
groupDescription	Beschreibung der Gruppe

Zusätzlich enthält die DSM-Schemazuordnung Felder, die keine Attributnamen sind. Dabei handelt es sich um die Namen der Objektklassen, die von DSM-basierten Anwendungen verwendet werden:

- Die GUI verwendet "computerMap", "groupMap" und "userMap", um die anzuzeigenden Knotentypen zu bestimmen.
- Der Verzeichnissynchronisierungsjob verwendet "userMap" und "computerMap".

Die DSM-Schemazuordnung enthält folgende Felder:

computerMap

Ordnet ein Objekt dem objectClass-Namen zu, der für einen Computer in dem konfigurierten Verzeichnis steht.

groupMap

Ordnet ein Objekt dem objectClass-Namen zu, der für eine Gruppe in dem konfigurierten Verzeichnis steht.

userMap

Ordnet ein Objekt dem objectClass-Namen zu, der für einen Benutzer in dem konfigurierten Verzeichnis steht.

containerMap

Ordnet ein Objekt dem Klassennamen für *Container* zu.

Active Directory-Schema

Die folgende Tabelle zeigt die Zuordnung der Active Directory-Attributnamen zum DSM-Schema:

DSM-Attributname	Active Directory-Attributname
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	sn
givenName	givenName
userName	name
displayName	displayName
userID	name

DSM-Attributname	Active Directory-Attributname
userPassword	userPassword
memberOf	memberOf
directReports	directReports
streetAddress	streetAddress
postalCode	postalCode
company	company
Abteilung	Abteilung
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	dnsHostName
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	member
groupDescription	description
containerMap	Container
groupMap	Gruppe
userMap	Anwender
computerMap	computer
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–
userDn*	distinguishedName
groupDn*	distinguishedName

DSM-Attributname	Active Directory-Attributname
assetDn*	distinguishedName
o*	o
ou*	ou

*** Hinweis:** Die Zuordnung dieser Attribute ist festgelegt und kann nicht geändert werden. Sie haben jedoch die Möglichkeit, diese DSM-Attributnamen in Abfragen zu verwenden.

Oracle Verzeichnis-Schema

Die folgende Tabelle zeigt die Zuordnung der Oracle Verzeichnis-Attributnamen zum DSM-Schema:

DSM-Attributname	Oracle Attributname
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	Sn
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	–
directReports	–
streetAddress	streetAddress
postalCode	postalCode
company	company
Abteilung	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	title

DSM-Attributname	Oracle Attributname
userDescription	description
assetCn	cn
assetName	name
dnsHostName	Host
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	member
groupDescription	description
containerMap	Container
groupMap	groupOfUniqueNames
userMap	inetOrgPerson
computerMap	computer
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–

*** Hinweis:** Die Zuordnung dieser Attribute ist festgelegt und kann nicht geändert werden. Sie haben jedoch die Möglichkeit, diese DSM-Attributnamen in Abfragen zu verwenden.

eTrust Directory-Schema

Die folgende Tabelle zeigt die Zuordnung der eTrust Directory-Attributnamen zum DSM-Schema:

DSM-Attributname	eTrust Directory-Attributname
objectClass	objectClass
dc	dc
c	c

DSM-Attributname	eTrust Directory-Attributname
l	l
userCn	cn
userSn	sn
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	–
directReports	–
streetAddress	streetAddress
postalCode	postalCode
company	company
Abteilung	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	Host
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	member
groupDescription	description
containerMap	Container

DSM-Attributname	eTrust Directory-Attributname
groupMap	groupOfNames
userMap	inetOrgPerson
computerMap	device
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–
userDn*	dn
groupDn*	dn
assetDn*	dn
o*	o

*** Hinweis:** Die Zuordnung dieser Attribute ist festgelegt und kann nicht geändert werden. Sie haben jedoch die Möglichkeit, diese DSM-Attributnamen in Abfragen zu verwenden.

NDS Directory-Schema

Die folgende Tabelle zeigt die Zuordnung der NDS-Attributnamen zum DSM-Schema:

DSM-Attributname	NDS-Attributname
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	Nachname
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	–
directReports	–
streetAddress	streetAddress

DSM-Attributname	NDS-Attributname
postalCode	postalCode
company	company
Abteilung	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	Host
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	member
groupDescription	description
containerMap	Container
groupMap	Gruppe
userMap	Anwender
computerMap	computer
uniqueComputerFields 1 – uniqueComputerFields 5	–
uniqueUserFields 1 – uniqueUserFields 5	–
userDn*	dn
groupDn*	dn
assetDn*	dn
o*	o
ou*	ou

*** Hinweis:** Die Zuordnung dieser Attribute ist festgelegt und kann nicht geändert werden. Sie haben jedoch die Möglichkeit, diese DSM-Attributnamen in Abfragen zu verwenden.

Verzeichnisintegration in CA IT Client Manager

CA ITCM unterstützt die folgenden Directory Services:

Hinweis: Unter Kompatibilitätsmatrix finden Sie eine aktualisierte Liste der unterstützten Verzeichnisintegrationsservices.

Directory Services unter Windows

Directory Service	Authentifizierung	Abfragen	Berichte	Bereitstellung	Remote Control-Rechte
Active Directory 2000	+	+	+	+	+
Active Directory 2003	+	+	+	+	+
OpenLDAP v2.0	+	+	+	+	+
OpenLDAP v2.1	+	+	+	+	+
OpenLDAP v2.2	+	+	+	+	+
Novell NDS	+	+	+	+	+
Novell eDirectory v8.5	+	+	+	+	+
eTrust Directory r8	+	+	+	+	+

Legende:

\+ = unterstützt

\- = wird nicht unterstützt

Directory Services unter Linux

Directory Service	Authentifizierung	Abfragen	Berichte	Bereitstellung	Remote Control-Rechte
Active Directory 2000	+	+	+	+	+
Active Directory 2003	+	+	+	+	+
OpenLDAP v2.0	+	+	+	+	+
OpenLDAP v2.1	+	+	+	+	+

Directory Service	Authentifizierung	Abfragen	Berichte	Bereitstellung	Remote Control-Rechte
OpenLDAP v2.2	+	+	+	+	+
Novell eDirectory v8.5	+	+	+	+	+
eTrust Directory r8	+	+	+	+	+

Legende:

+ = unterstützt

Kapitel 11: CA ITCM-Sicherheitsfunktionen

Die Sicherheitsfunktionen in CA ITCM umfassen zwei Bereiche.

Authentifizierung

Bietet die Sicherheit, dass das anfordernde Objekt auch ist, was es vorgibt.

Autorisierung

Bietet die Konfiguration und Validierung der Zugriffrechte und Berechtigungen zum Durchführen von Vorgängen für gesicherte Objekte.

Dieses Kapitel enthält folgende Themen:

Authentifizierung (siehe Seite 403)
Autorisierung (siehe Seite 415)
Konfigurieren von Common Security (siehe Seite 436)
Unterstützung der Sicherheitsbereiche (siehe Seite 444)
Konfigurieren der Verschlüsselung (siehe Seite 448)
FIPS-konforme Kryptographie (siehe Seite 452)

Authentifizierung

Die Authentifizierung identifiziert Mitglieder einer Trusted Computing Base auf Grundlage der angegebenen Anmeldeinformationen.

Mitglieder einer Trusted Computing Base sind:

Benutzer, und indirekt Gruppenmitgliedschaft

In erster Linie handelt es sich hierbei um homogene Sicherheitsprinzipale aus dem aktuellen Betriebssystem. Beispielsweise können dies Windows-Benutzer (Active Directory, Domäne oder lokal), UNIX- (LDAP) oder lokale UNIX-Benutzer sein.

Rechner

Computer, die zu einer Trusted Computing Base (TCB) gehören, z. B. Windows NT, können identifiziert und authentifiziert werden. Es ist theoretisch möglich, dass UNIX-Computer identifiziert werden, da auch sie zu einer Trusted Computing Base gehören, mit der ein Vertrauensverhältnis eingerichtet werden kann.

Die folgenden Informationen werden zum Authentifizieren eines Benutzers oder Computers verwendet.

- In Windows-Betriebsumgebungen:
  - Benutzername:
  - Kennwort
  - Windows-Domäne
  - Sicherheitsprovider
- In Linux- und UNIX-Betriebsumgebungen:
  - Computername
  - Benutzername:
  - Kennwort
  - Sicherheitsprovider

Für unterschiedliche Anwendungen gelten auch unterschiedliche Anforderungen zur Authentifizierung. Wenn möglich, wird eine implizite Anmeldung verwendet. D. h., der Benutzer wird nicht aufgefordert, explizite Anmeldeinformationen einzugeben, sondern die aktuellen Anmeldeinformationen des Benutzers werden implizit verwendet.

In einigen Fällen sind die Anmeldeinformationen jedoch für die Ressource, auf die sie zugreifen, nicht gültig. Auch für spezielle Vorgänge kann eine erneute Authentifizierung erforderlich sein. Wenn keine implizite Anmeldung verwendet werden soll oder die Anmeldeinformationen nicht gültig sind, kann eine GUI-Anwendung bei Bedarf zur Eingabe der Anmeldeinformationen auffordern. Eine Befehlszeilenanwendung im Batch-Modus schlägt jedoch fehl und zeichnet einen Authentifizierungsfehler auf.

Wenn Sie einen LDAP-Sicherheitsprovider verwenden, um beim Angeben der Anmeldeinformationen Benutzer anhand eines Verzeichnisses zu authentifizieren, müssen Sie sicherstellen, dass die Anmeldeinformationen für das Zielverzeichnis gültig sind und vollständig angegeben werden. Verwenden Sie für ein Active Directory die vollständige LDAP DN-Option, beispielsweise:

```
CN=user,OU=Users,OU=myOU,DC=mydomain,DC=com
```

Wenn Sie externe generische LDAP-Verzeichnisse zur Authentifizierung verwenden, müssen den authentifizierenden Objekten direkte Zugriffsrechte erteilt werden, da eine Gruppenzugehörigkeit nicht direkt evaluiert werden kann. Dies gilt nicht für Active Directory.

Unterstützte Formate für Benutzernamen

Die folgenden Formate für Benutzernamen werden von CA ITCM unterstützt. Diese Namensformate gelten für alle CA Technologies-Anwendungen, die einen Benutzernamen erfordern, z. B. für die Explorer-GUI und die Webdienste.

Systemeigene Sicherheit von Windows oder lokale Sicherheit von Linux/UNIX (d. h. lokale Benutzer und vertrauenswürdige Domänen)

Format des Benutzernamens: *Benutzername* (Windows NT-Vorgängerformat oder Linux-Benutzer)

Datenaustausch zwischen LDAP und Active Directory (Windows und Linux/UNIX)

Format des Benutzernamens: UPN oder DN

Datenaustausch zwischen LDAP und einem Verzeichnis (ausgenommen Active Directory) (Windows und Linux/UNIX)

Format des Benutzernamens: DN

Format des Benutzernamens: UID oder SN (für Oracle LDAP)

NDS-Verzeichnis (nur Windows)

Format des Benutzernamens: DN

X.509-zertifikatbasierte Authentifizierung

Wenn ein CA ITCM-Client-Prozess eine Verbindung zu einem CAF-Plug-in herstellt, das eine Authentifizierung erfordert, muss der Client-Prozess die Sicherheitsinformationen für die Sicherheitsanforderungen der Zieldienste übergeben. Wenn der Client-Prozess als autonomer Prozess ausgeführt wird, z. B. als Windows NT-Dienst oder UNIX-Daemon, kann der Client-Prozess die Authentifizierung mit den X.509 V3-Zertifikaten ausführen, wenn keine Benutzerinformationen vorliegen.

Ein X.509-Zertifikat für die CA ITCM-Authentifizierung besteht aus einer Reihe von Attributswertpaaren, die mit dem öffentlichen Codierungsschlüssel eines asymmetrischen Schlüsselpaars verpackt werden. Das Zertifikat wird von einem Root-Zertifikat digital signiert und versiegelt. Das Zertifikat zeichnet den Namen des Subjekts, für das das Zertifikat ausgestellt wurde, den Namen der ausstellenden Zertifizierungsstelle und die Ablaufinformationen auf. Der Subjektname wird häufig auch als "DN" (Distinguished Name) bezeichnet. Der Subjektname wird einer Uniform Resource Identifier (URI) im x509cert-Namespace zugeordnet, z. B.:

```
x509cert://dsm r11/CN=Basic Host Identity,O=Computer Associates,C=US
```

Eine Übersicht der aktuellen Zertifikate finden Sie unter Allgemeine Zertifikate (siehe Seite 579) und Anwendungsspezifische Zertifikate (siehe Seite 580).

Bei Verwendung von Kryptographie mit öffentlichem Schlüssel authentifizieren sich die Clients auf Anforderung bei Scalability-Servern selbst. Ein Scalability-Server kann anschließend mit der zertifizierten Identität die folgenden Autorisierungsprüfungen ausführen und Überwachungsdatensätze übergeben. Über die Managementkonsole können Sie den Zertifikat-URIs Berechtigungen für Tasks oder Objekte in der CA ITCM-Management-Datenbank zuweisen.

Sicherheit auf Objektebene und Zertifikate

Die CA ITCM-Management-Datenbank bietet Sicherheit auf Klassen- und Objektebene (Object Level Security, OLS). Die in der Datenbank zugewiesenen Berechtigungen sind einem Sicherheitsprofil zugeordnet, das durch eine Objekt-URI dargestellt wird. Zertifikat-URIs können Sicherheitsprofilen zugeordnet und damit zum Regulieren des Zugriffs auf die CA ITCM-Management-Datenbank verwendet werden.

Beispielsweise authentifizieren sich Scalability-Server beim Verbindungsaufbau zu einem Domänen-Manager mit einem Registrierungszertifikat selbst. Die dem Registrierungszertifikat zugeordnete URI wurde mit Berechtigungen für die Datenbank ausgestattet, die nur die Registrierung des Scalability-Serverknotens zulassen.

Root-Zertifikate

CA ITCM verwendet vertrauenswürdige Root-Zertifikate zum Validieren der Zertifikate, die in der Authentifizierung verwendet werden. Sie können mehrere Root-Zertifikate parallel verwenden, um das Management unterschiedlicher Berechtigungsketten zu ermöglichen oder um die Migration von einer Zertifikatskette zu einer neuen Kette zu unterstützen.

Damit zwei Knoten erfolgreich miteinander kommunizieren und anschließend authentifizieren können, benötigt der Authentifizierungsknoten (Responder) Zugriff auf das Root-Zertifikat, mit dem das Zertifikat der authentifizierenden Partei signiert wurde (Initiator). Wenn das Zertifikat nicht verfügbar ist, nicht erkannt wird oder anderweitig ungültig ist, schlägt die Authentifizierung fehl. Während einer geplanten Zertifikatmigration kann der Authentifizierungsknoten mit einem oder mehreren Root-Zertifikaten aktualisiert werden, um die in Phasen unterteilte Migration von Clients zu ermöglichen. Initiatoren mit unterschiedlichen Zertifikatversionen authentifizieren weiterhin erfolgreich, wenn sie von Root-Zertifikaten signiert sind, die vom Responder als vertrauenswürdig eingestuft werden.

Zertifikatspeicher

Die Authentifizierungszertifikate werden gesichert auf jedem CA ITCM-Knoten gespeichert. Die Zertifikatdateien sind kennwortgeschützt. Das Verwendungskennwort wird mit der CA ITCM-Konfiguration verschlüsselt.

Basis-Hostidentitätszertifikate

Jeder CA ITCM-Knoten verfügt über ein Zertifikat, in dem die Basis-Hostidentität (BHI) standardmäßig installiert ist. Andere Zertifikate für spezielle Zwecke werden mit den Diensten installiert, die diese Zertifikate erforderlich machen (Informationen finden Sie unter "Aktuelle Zertifikate" (siehe Seite 579)). Die CA IT Client Manager-Installation wird mit einem Standardzertifikat geliefert, das mit einem CA ITCM-Root-Zertifikat signiert ist. Dieses Zertifikat wird auf jedem CA ITCM-Knoten des Unternehmens installiert.

Es wird empfohlen, dass Endbenutzer das Erstellen ihrer eigenen Root-Zertifikate, Basis-Hostidentitätszertifikate (BHI) und der anwendungsspezifischen Zertifikate planen. Informationen zum Ersetzen der Standardzertifikate durch spezielle Zertifikate des Endbenutzers finden Sie unter "So importieren Sie Ihre eigenen X.509-Zertifikate in das Installations-Image (siehe Seite 229)".

Beim Erstellen neuer BHI-Zertifikate sind drei primäre Paradigmen zu beachten:

- Erstellen Sie ein einzelnes Hostidentitätszertifikat, das auf allen CA ITCM-Knoten des Enterprises verwendet wird. Dies ist die einfachste Lösung, da das benutzerdefinierte Installations-Image nur einmal erzeugt werden muss, um ein auf die Anforderungen abgestimmtes Paket zu erstellen.

- Erstellen eines eindeutigen Hostidentitätszertifikats für jeden Knoten im DSM-Enterprise. Dies ist die komplexeste Lösung. Der DN, der jedem Knoten zugewiesen wird, muss eindeutig sein und die Identität des Hostrechners wiedergeben. Ein vollständig qualifizierter Hostname reicht üblicherweise aus. Sie benötigen ein benutzerdefiniertes Installations-Image, um die entsprechende Zertifikatdatei auf dem Zielrechner zu installieren.
- Eine Kombination aus den beiden oben genannten Paradigmen. Erstellen Sie ein einzelnes Hostidentitätszertifikat, das auf den meisten CA ITCM-Knoten verwendet wird. Erstellen Sie auf die Anforderungen abgestimmte Zertifikate zur Verwendung auf dem DSM-Scalability-Server und auf den Managerknoten. Wenn Sie eine Anforderung für ein angepasstes Zertifikat ermittelt haben, stellen Sie ein neues Zertifikat aus und installieren es auf dem angegebenen Knoten. Dies ist die flexibelste Lösung. Wichtige Knoten im Unternehmen werden effizienter identifiziert und geschützt.

Zertifikatverteilung

Wie die Zertifikate verteilt werden sollen, muss bereits vor der Zertifikaterstellung bekannt sein. Die Verteilung von Zertifikaten kann je nach der gewählten Methode (siehe Beschreibung unter "Basis-Hostidentitätszertifikate (siehe Seite 407)") zum Erstellen von Zertifikaten recht komplex sein.

CA ITCM bietet keine automatische Erstellung von Zertifikaten. Zum Lieferumfang gehören Standardzertifikate für jeden CA ITCM-Knoten und anwendungsspezifische Zertifikate.

Nach einer Standardinstallation ist eine Migration von den Standardzertifikaten zu anderen Zertifikaten möglich. Die Zertifikate können auf folgende (vereinfachte) Weise verteilt werden. Aufgrund der parallelen Verwendung vertrauenswürdiger Root-Zertifikate wird eine erfolgreiche vertrauenswürdige Migration ohne Ausfall bei der Kommunikation und Authentifizierung möglich.

1. Erstellen Sie ein neues Root-Zertifikat. Stellen Sie sicher, dass der Root-Name (DN) nicht mit dem Namen des vorhandenen CA ITCM-Root-Zertifikats übereinstimmt.
2. Planen Sie die Verteilung des neuen DER-codierten Root-Zertifikats auf alle Knoten der CA ITCM-Infrastruktur. Damit wird der Root als vertrauenswürdige Root-Berechtigung auf allen CA ITCM-Knoten aktiviert.
3. Erstellen Sie neue Sicherheitsprofile in der CA ITCM-Management-Datenbank, um die vorhandenen anwendungsspezifischen Zertifikatprofile zu ersetzen. Löschen Sie alte Profile noch nicht.
4. Planen Sie die Verteilung der neuen Zertifikate auf alle CA ITCM-Knoten.

5. Wenn die Zertifikatverteilung erfolgreich war, planen Sie das Löschen der alten CA ITCM-Zertifikate.
6. Löschen Sie die alten Sicherheitsprofile für die anwendungsspezifischen Zertifikate.

Diese Liste ist nicht vollständig: Informationen zu umfangreichen Zertifikatverteilungen und/oder Ersatz durch eine vollständige PKI-Implementierung erhalten Sie vom Technischen Support von CA Technologies.

Erstellen neuer Zertifikate

Zum Erstellen neuer Zertifikate können Sie das mitgelieferte Tool "cacertutil" verwenden oder mit einem bestehenden PKI Zertifikate erzeugen. Die Verwendung externer PKI-Systeme übersteigt den Rahmen dieser Dokumentation. Aber die Zertifikatanforderungen stimmen mit den Anforderungen für eine Zertifikaterstellung mit cacertutil überein.

Hinweis: Ein bestehender PKI müsste ein neues Root-Zertifikat für die CA ITCM-Infrastruktur erstellen.

Erstellen eines neuen Root-Zertifikats

Wenn Sie ein neues Root-Zertifikat erzeugen, müssen die folgenden beiden Formen des Zertifikats erstellt werden:

- Eine PKCS#12-codierte Datei. Sie enthält den öffentlichen Abschnitt des Zertifikats und den privaten Schlüssel.
- Eine DER-codierte Datei. Sie enthält lediglich den öffentlich zugänglichen Abschnitt des Zertifikats.

Beide Formen des Zertifikats werden zur gleichen Zeit wie das CA ITCM-Tool erzeugt. Wenn Sie eine externe PKI verwenden, kann das Root-Zertifikat in das DER-Format exportiert werden.

Das neue Root-Zertifikat ist von zentraler Bedeutung für die Sicherheit in CA ITCM. Daher muss es gegen versehentliche oder mutwillige Veröffentlichung geschützt werden. Die PKCS#12-Zertifikatdatei muss mit komplexem Kennwortschutz ausgestattet und in einem sicheren Verwaltungsdatenspeicher gespeichert werden.

Mit dem Zertifikat im PKCS#12-Format werden andere Zertifikate signiert. Mit dem Zertifikat im DER-Format werden diese signierten Zertifikate geprüft.

Der Befehl zum Erstellen eines neuen Root-Zertifikats hat folgendes Format:

```
cacertutil create -o:rootname.p12 -od:rootname.der -op:passphrase “-
s:CN=YourRoot,O=YourOrg,C=Country” -d:NumberOfDays -oe
```

-o

Gibt die Ausgabe *Dateiname* für das PKCS#12-verpackte Zertifikat an.

-od

Gibt die Ausgabe *Dateiname* für das DER-codierte Zertifikat an.

-op

Gibt ein Kennwort zur Verschlüsselung der PKCS#12-Zertifikatdatei an.

-s

Legt das Subjekt des Zertifikats fest.

-d

Gibt die Lebensdauer des Zertifikats in Tagen an (z. B. 730 (= 2 Jahre)).

-oe

Erzeugt eine nach dem Zufallsprinzip verschlüsselte Version des Kennworts, mit dem das Zertifikat verschlüsselt und auf der Konsole ausgegeben wird. Dieses verschlüsselte Kennwort kann dem Zertifikat-Tool statt eines Nur-Text-Kennworts bereitgestellt werden.

Erstellen anwendungsspezifischer Zertifikate

Erstellen Sie für jede unter "Aktuelle Zertifikate (siehe Seite 579)" aufgeführte Anwendung ein neues Zertifikat. Wenn Sie nicht den DN in der Tabelle des Anhangs verwenden, müssen Sie auch die erforderlichen Berechtigungen für das Zertifikatsicherheitsprofil im CA ITCM-Sicherheitsbrowser zuweisen.

Um sicherzustellen, dass das neu erstellte Zertifikat für den CA ITCM-Sicherheitsbrowser sichtbar ist, muss das DER-codierte Zertifikat in die CA ITCM-Zertifikatdatenbank auf den Managerknoten importiert werden.

Die neuen Zertifikate werden mit folgendem Befehl erstellt:

```
cacertutil create -o:certname.p12 -od:certname.der -op:passphrase “-s:CertDN” -
i:rootname.p12 -ip:rootpassphrase -d:730
```

-o

Gibt den Ausgabedateinamen für das PKCS#12-verpackte Zertifikat an.

-od

Gibt den Ausgabedateinamen für das DER-codierte Zertifikat an.

-op

Gibt das Kennwort zum Schutz des PKCS#12-Ausgabezertifikats an.

-s

Gibt den DN an, für den das Zertifikat ausgestellt wird.

-i

Gibt den Dateinamen des PKCS#12-Root-Zertifikats an.

-ip

Gibt das Kennwort zum Schutz des PKCS#12-Root-Zertifikats an.

-d

Gibt die Lebensdauer des Zertifikats in Tagen an (im Beispiel zwei Jahre (= 730 Tage)).

Erstellen des Basis-Hostidentitätszertifikats

Das Basis-Hostidentitätszertifikat (BHI-Zertifikat) verfügt nicht über Berechtigungen in der CA ITCM-Management-Datenbank und kein zugeordnetes Sicherheitsprofil in der Standardinstallation. Daher müssen im Rahmen eines neuen DN für das Zertifikat die CA ITCM-Sicherheitsprofile und Berechtigungen nicht angepasst werden.

Dem BHI-Zertifikat wird folgender Standard-DN zugeordnet:

CN=Basic Host Identity,O=Computer Associates,C=US

Der Befehl zum Erstellen eines neuen Basis-Hostidentitätszertifikats hat folgendes Format:

```
cacertutil create -o:certname.p12 -od:certname.der -op:passphrase “-s:CertDN” -
i:rootname.p12 -ip:rootpassphrase -d:730
```

-o

Gibt den Ausgabedateinamen für das PKCS#12-verpackte Zertifikat an.

-od

Gibt den Ausgabedateinamen für das DER-codierte Zertifikat an.

-op

Gibt das Kennwort zum Schutz des PKCS#12-Ausgabezertifikats an.

-s

Gibt den DN an, für den das Zertifikat ausgestellt wird.

-i

Gibt den Dateinamen des PKCS#12-Root-Zertifikats an.

-ip

Gibt das Kennwort zum Schutz des PKCS#12-Root-Zertifikats an.

-d

Gibt die Lebensdauer des Zertifikats in Tagen an (im Beispiel zwei Jahre (= 730 Tage)).

Installieren neuer Zertifikate

Wenn Sie auf einem CA ITCM-Knoten neue Zertifikate installieren, muss dies unter Windows von einem lokalen Administrator, d. h. einem Mitglied der Administratorgruppe, ausgeführt werden.

Installieren eines neuen Root-Zertifikats

Zum Erstellen eines neuen Stammprüfungszertifikats auf einem CA ITCM-Knoten verwenden Sie die DER-codierte Datei. Der Befehl zum Installieren dieses Zertifikats hat folgendes Format:

```
cacertutil import -i:rootcert.der -ip:passphrase -it:X509V3
```

Damit werden die öffentlich zugänglichen Informationen des Zertifikats als vertrauenswürdiges Root-Zertifikat in die Zertifikatdatenbank importiert.

Installieren anwendungsspezifischer Zertifikate

In der CA IT Client Manager-Code-Basis wird mit einem Tag-Namen auf die anwendungsspezifischen Zertifikate verwiesen, jedoch nicht mit dem DN, der den Zertifikaten zugewiesen ist. Die entsprechenden Tag-Namen werden unter "Aktuelle Zertifikate (siehe Seite 579)" dargestellt. Dieses Zertifikat kann nur auf Knoten installiert werden, die das Zertifikat zum Authentifizieren bei einem DSM-Scalability-Server oder Manager benötigen.

Der Befehl zum Installieren eines anwendungsspezifischen Zertifikats hat folgendes Format:

```
cacertutil Import -i:certname.p12 -ip:passphrase -t:tagname
```

-i

Gibt den Namen des PKCS#12-Zertifikats an, das Sie importieren möchten.

-ip

Gibt das Kennwort zum Schutz des Zertifikats an.

-t

Gibt den Tag-Namen des Zertifikats an.

Damit das Zertifikat für den DSM-Sicherheitsbrowser sichtbar wird, muss das DER-codierte Zertifikat in die Zertifikatdatenbank auf den Managerknoten importiert werden. Der Befehl zum Erstellen eines DER-codierten Zertifikats hat folgendes Format:

```
cacertutil import -i:certname.der -it:X509V3
```

-i

Gibt den Namen des DER-codierten Zertifikats an, das Sie importieren möchten.

-it

Gibt den Typ des Zertifikats an, das importiert werden soll. X509V3 gibt die DER-Kodierung an.

Installieren des Basis-Hostidentitätszertifikats.

Das Basis-Hostidentitätszertifikat wird immer mit dem Tag-Namen "dsmcommon" installiert. Der Befehl zum Installieren des BHI-Zertifikats hat folgendes Format:

```
cacertutil import -i:certname.p12 -ip:passphrase -t:dsmcommon -h
```

-i

Gibt den Namen der PKCS#12-Eingabezertifikatdatei an.

-ip

Gibt das Kennwort zum Schutz des Eingabezertifikats an.

-t

Gibt den Tag-Namen des Zertifikats an.

-h

Gibt an, dass mit dem Zertifikat die Standardhostidentität angegeben werden soll.

Ersetzen von Zertifikaten

Damit die standardmäßigen CA ITCM-Zertifikate ersetzt werden können, müssen alle neuen Zertifikate dieselben physischen Dateinamen wie die Originale aufweisen. Die den Zertifikaten zugewiesenen Subjektnamen müssen nicht dem Original entsprechen. Diese werden von der Installationsdatei "cfcert.ini" aufgezeichnet und gesteuert und während der Installation entsprechend den Anweisungen in dieser Datei in die Datenbank eingefügt.

Die folgende Tabelle enthält eine Liste der Dateinamen und der entsprechenden Zuordnungen:

Dateiname	Zugeordnet zum CA ITCM-Thema
itrm_dsm_r11_root.der	Stammzertifikat
basic_id.p12	Basis-Hostidentitätszertifikat
dsmpwchgent.p12	Enterprise-Zugriff
dsmpwchgdom.p12	Domänenzugriff
dsmpwchgrep.p12	Reporter-Zugriff
ccsm.p12	Zugriff auf CSM
itrm_dsm_r11_cmdir_eng.p12	Zugriff auf Verzeichnissynchronisierung
registration.p12	Zugriff auf Registrierung
itrm_dsm_r11_sd_catalog.p12	Zugriff auf SD-Katalog
itrm_dsm_r11_agent_mover.p12	Zugriff auf SD-Agent-Mover

Entfernen eines Zertifikats

Zertifikate können jeweils einzeln oder gemeinsam entfernt werden.

Um ein einzelnes Zertifikat zu entfernen, geben Sie folgenden Befehl ein:

```
cacertutil remove -s:Subjektname [-t:Tagname] [-l:{local|global}]
```

-s

Gibt den Namen des Subjekts an, für das das Zertifikat ausgestellt wurde.

-t

Gibt den Tag-Namen des Zertifikats an, wenn es mit einem Tag-Namen installiert wurde.

-l

Gibt an, ob das Zertifikat im globalen oder lokalen allgemeinen Datenspeicher gespeichert wurde.

Alle Zertifikate werden mit folgendem Befehl entfernt:

```
cacertutil flush
```

Wichtig! Mit diesem Befehl werden alle Zertifikateinträge für den aktuellen Benutzer und den lokalen Rechner aus dem allgemeinen Datenspeicher entfernt (wenn die Rechte des aktuellen Prozessbenutzers ausreichen).

VMware-ESX-Sicherheit und Authentifizierung

Der CA ITCM-AM-Remote-Agent unterstützt nur VMware-ESX-SERVER, die in sicherem HTTP-Modus ausgeführt werden. VMware empfiehlt, sicheres HTTP (HTTPS, die Standardkonfiguration) für die Produktionsbereitstellung zu verwenden. Daher verbindet der AM Remote-Agent sich nur mit ESX-Hosts, die die empfohlene Standardkonfiguration mit sicherem HTTP verwenden.

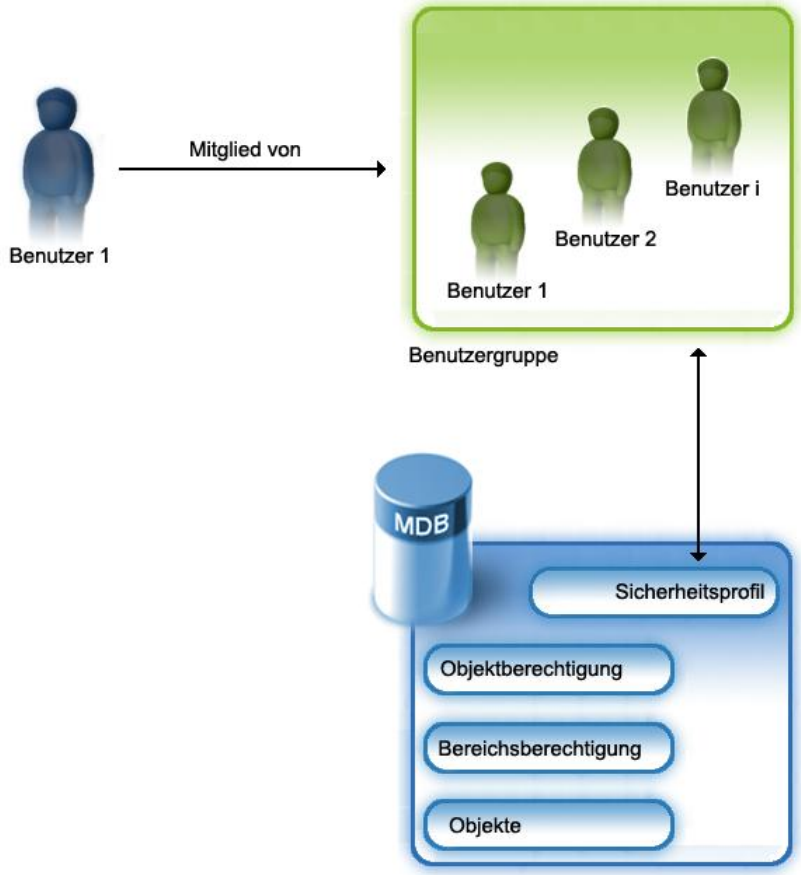
Secure Sockets Layer (SSL) wird als Verbindungsprotokoll zwischen dem DSM-Agenten und den ESX-Hostrechner verwendet. Weil die Identität eines ESX-Hostrechners nicht im Voraus bekannt ist, gibt es allerdings keine Authentifizierung zwischen dem DSM-Agenten und dem ESX-Host. Zertifikate werden nicht zur Authentisierung eines ESX-Hosts verwendet.

Autorisierung

Die Autorisierung steuert die Rechte und Berechtigungen für ein Objekt, das einer authentifizierten Entität zugeordnet ist. Üblicherweise ist dies ein angemeldeter Benutzer. Authentifizierte Entitäten werden von Sicherheitsprofilen verwaltet. Einem Benutzer oder einer Benutzergruppe entspricht ein Sicherheitsprofil, über das alle Berechtigungen verwaltet werden.

Das Sicherheitsuntersystem von CA ITCM verwaltet die Autorisierung mit Hilfe einer soliden und generischen Sicherheitsoption für alle Komponenten von CA IT Client Manager. Diese steuert die Rechte und Berechtigungen für ein Objekt, das einer authentifizierten Entität zugeordnet ist, die als Sicherheitsprofil bezeichnet wird.

Die folgende Abbildung bietet eine Übersicht über das Sicherheitsuntersystem zur Steuerung der Autorisierung:



Beim System angemeldete Benutzer sind normalerweise Mitglied mindestens einer Benutzergruppe. Die Benutzergruppe entspricht einem Sicherheitsprofil.

Der CA ITCM-Administrator ist also für die Erstellung des Sicherheitsprofils für eine Benutzergruppe oder eines eigenen Sicherheitsprofils für einen bestimmten Benutzer verantwortlich.

Neben den CA ITCM-Objekten werden die Berechtigungen für die Sicherheitsprofile hinsichtlich der Objekte in der MDB gespeichert.

Sie können beispielsweise Sicherheitsprofile erstellen, um festzulegen, welche vom Betriebssystem abhängigen Gruppen und Benutzer auf das CA ITCM-System zugreifen können. Außerdem können Sie Klassenberechtigungen sowie Gruppen- und Objektberechtigungen einrichten und den Zugriff von Benutzern oder Benutzergruppen auf bestimmte Ordner oder Objekte einschränken.

Sicherheitsprofile

Ein Sicherheitsprofil ist ein Benutzerkonto in einem Betriebssystem oder eine Gruppe in einem Domänen-Manager (lokale Profile) oder in der Netzwerkdomäne (Domänenprofil).

Das Sicherheitsuntersystem von CA ITCM unterstützt zahlreiche Sicherheitsprofile. Sicherheitsprofile sind entweder integriert (d. h., sie werden bei der Installation erstellt) oder benutzerdefiniert.

Benutzerdefinierte Sicherheitsprofile entsprechen entweder einem einzelnen Benutzer oder einer Benutzergruppe.

Bei der Installation werden unter anderem die folgenden wichtigen Sicherheitsprofile erstellt:

- Eigentümer (virtuelles Konto)
- Jeder (standardmäßiges virtuelles Konto für jeden)

Neben dem Sicherheitsprofil gibt es eine Reihe von Sicherheitsklassen, die einem Profil zugeordnet werden. Jedes Profil verfügt über eine eigene Gruppe von Sicherheitsklassen. Mit Hilfe einer Sicherheitsklasse können Sie die Berechtigungen festlegen, die einer Instanz einer solchen Klasse bei ihrer Erstellung zugewiesen werden.

Sie können auch Sicherheitsprofile für Benutzer in den vertrauenswürdigen Domänen erstellen. Jeder Benutzer benötigt ein gültiges Sicherheitsprofil für die Anmeldung beim System. Wenn einer verwalteten Gruppe neue Benutzer hinzugefügt werden, übernehmen sie automatisch die der Gruppe zugewiesenen Zugriffsrechte und können sich sofort beim System anmelden.

Ein Benutzer kann mehrere Profile haben. Jedes Profil kann jedoch nur einem Benutzer oder einer Gruppe zugeordnet werden. Wenn ein Benutzer beispielsweise Mitglied einer Gruppe ist, kann er zwei Profile haben: Ein Profil ist dem Benutzerkonto zugeordnet, das andere Profil ist der Gruppe zugeordnet. In diesem Fall hat der Benutzer die (mathematische) Vereinigungsmenge der Berechtigungen in beiden Profilen.

Wenn ein Benutzer Mitglied in mehreren Sicherheitsprofilen ist, entspricht die gültige Berechtigung für diesen Benutzer einer (mathematischen) Vereinigungsmenge jeder der Einzelberechtigungen, die für jedes Sicherheitsprofil festgelegt wurden (wie eine logische OR-Verknüpfung aller Berechtigungen).

Wenn Sie dem Benutzer eines einzelnen Sicherheitsprofils den Zugriff verweigern möchten, müssen Sie diesen Benutzer aus dem Sicherheitsprofil entfernen.

Das System enthält vordefinierte Sicherheitsprofile. Zusätzlich können Sie im Dialogfeld "Sicherheitsprofile" eine beliebige Anzahl von Profilen erstellen.

Es wird empfohlen, dass mindestens einem dieser Profile Vollzugriff auf das System gewährt wird.

Übersicht über Berechtigungen

Unter die Autorisierung fallen die folgenden Berechtigungstypen:

- Klassenberechtigungen
- Objektberechtigungen
- Bereichsberechtigungen

Das Sicherheitsuntersystem verwaltet alle Berechtigungstypen und wendet beim Abrufen der gültigen Berechtigungen eine kumulative Vorgehensweise an.

Wenn Sie die Bereichsberechtigungen aktiviert haben, wird beiden Berechtigungstypen (Objekt- und Bereichsberechtigungen) Zugriff auf die Objekte zugewiesen. Ein Benutzer benötigt für die Verwaltung eines Objektes also Objektberechtigungen *und* Bereichsberechtigungen. Objektberechtigungen werden nur aktiviert, wenn die Unterstützung der Bereiche deaktiviert ist.

Klassenberechtigungen

Klassenberechtigungen sind die Zugriffsrechte, die Sie auf Klassenebene festlegen. Dies bedeutet, dass die Berechtigungen auf Klassenebene den Standardrechten für jedes Objekt entsprechen, das eine Instanz dieser Klasse ist.

Beim Erstellen von Sicherheitsprofilen müssen Sie die Klassenberechtigungen für jedes Sicherheitsprofil festlegen. Für alle Sicherheitsklassen ist standardmäßig "Kein Zugriff" festgelegt. Sicherheitsprofile mit entsprechenden Klassenberechtigungen gewähren Ihnen Zugriffsrechte für das System. Dies können Sie im Dialogfeld "Klassenberechtigungen angeben.

Klassenberechtigungen gelten global für alle Objekte einer Objektklasse. Über das Dialogfenster "Objektberechtigungen" bzw. das Dialogfeld "Sicherheitsgruppenberechtigungen" können Sie den Zugriff von Benutzern auf ein bestimmtes Objekt oder einen bestimmten Ordner im Explorer einschränken oder erweiterte Zugriffsrechte gewähren.

Sicherheitsklassen werden zur Gruppierung von Objekten desselben Typs verwendet. Das Sicherheitsuntersystem von CA IT Client Manager unterstützt die folgenden Sicherheitsklassen:

- Erkannte Hardware (Computer)
- Benutzer
- Computerbenutzer
- Manager
- Server
- Asset-Gruppen
- Servergruppen
- Domänengruppen
- Abfragen
- Sicherheitsklassen
- Sicherheitsprofile
- Softwarepakete
- Softwareprozeduren
- Prozedurgruppen
- Jobcontainer
- Softwarejobs
- Asset-Jobs
- Module
- Abfragebasierte Richtlinien
- Ereignisbasierte Richtlinien
- OSIM-Boot-Images
- OSIM-BS-Images
- Engine
- Computer für Konfigurationsrichtlinien
- Benutzer für Konfigurationsrichtlinien
- Zugriff auf externe Verzeichnisse
- Berichtsvorlagen
- Inventarmodule

Die folgenden Sicherheitsklassen werden nur auf Klassenebene verwendet:

- MDB-Zugriff
- Systemsteuerung aktivieren
- Remote Control aktivieren

Sicherheit auf Klassenebene bedeutet, dass alle Objekte oder Instanzen einer Klasse die standardmäßig für die Klasse definierten Berechtigungen erhalten.

Für bestimmte Aktionen erforderliche Kombinationen aus Klassenberechtigungen

Einige Rechte von Objektklassen hängen voneinander ab, d. h., wenn Sie die folgenden Aktionen durchführen möchten, müssen Sie mehreren Objektklassen Rechte zuweisen.

Berichtsvorlagen

Wenn Sie eine Berichtsvorlage planen möchten, müssen Sie den Objektklassen "Berichtsplanung" *und* "Engine" Änderungsrechte zuweisen.

Sicherheitsprofile

Die Sicherheitsklasse "Sicherheitsprofile" steuert die Verarbeitung mit Hilfe von Sicherheitsprofilen (Löschen usw.). Wenn Sie die Objektklassenberechtigungen eines Sicherheitsprofils ändern möchten, benötigen Sie speziellen Zugriff (VRP mit der Berechtigung 'P') auf die Objektklasse "Klassenberechtigungen".

Engine

Wenn Sie einen Engine-Task mit einer Engine verknüpfen möchten, müssen Sie der Objektklasse "Engine" die Berechtigung zum Ändern *und* der Objektklasse "Engine-Task" die Berechtigung zum Verwalten zuweisen.

Wenn Sie, hinsichtlich der Engine-Sicherheit, Engine-Objekte starten, beenden oder ändern möchten, müssen Sie der Klasse "Engine" im Sicherheitsprofil das Recht zum Vollzugriff *und* dem Computer, auf dem die Engine ausgeführt wird, höhere Rechte als die des NT-Administrators oder Root-Rechte zuweisen.

Sicherheit von Softwarejobs

Wenn Sie einen Softwarejob im Ordner "/computer" ändern oder entfernen möchten, wird die Software an "/Jobs/Softwarejobs" geliefert, und die Objektklassen "Computer" und "Softwarejob" benötigen Rechte zum Ändern.

Prozedursicherheit

Wenn Sie Prozedurobjekte starten, beenden oder ändern möchten, müssen Sie der Klasse "Prozedur" die Berechtigung "Ändern (VRXWD)" *und* höhere Berechtigungen als Dateiberechtigungen für den Administrator oder Root zuweisen.

Unterstützung der Sicherheitsbereiche

Wenn Sie die Unterstützung für Sicherheitsbereiche deaktivieren oder aktivieren und Standard-Sicherheitsbereiche definieren möchten, müssen die Klassenberechtigungen für die Objektklasse "Sicherheitsbereich" mindestens auf "Spezieller Zugriff" (VP) festgelegt werden.

Wenn Sie Sicherheitsprofile mit einem Sicherheitsbereich verknüpfen möchten, genügt die Berechtigung "Anzeigen" (V) für die Objektklasse "Sicherheitsbereich". Die Klassenberechtigungen für die Objektklasse "Sicherheitsprofile" muss mindestens auf "Spezieller Zugriff" (VW) festgelegt werden.

Objektberechtigungen

Das Einstellen der Objektberechtigungen ist hilfreich, wenn Sie den Zugriff auf ein bestimmtes Objekt einschränken möchten. Standardmäßig übernehmen alle Objekte die Berechtigungen, die für die Objektklasse eingestellt sind.

Objektberechtigungen haben Vorrang vor Klassen- und Gruppenberechtigungen.

Objektberechtigungen sind immer vorhanden. Sie werden vom Sicherheitsuntersystem verwaltet und können nicht deaktiviert werden. Wenn Sie die Objektberechtigungen nicht verwalten möchten, können Sie die Berechtigungen auf Klassenebene für alle Sicherheitsebenen auf "Vollzugriff" setzen.

Die Autorisierung basiert auf dem Konzept "Zugriffssteuerungseintrag" ("Access Control Entry" ACE). Ein ACE besteht aus einer beliebigen Kombination der Codebuchstaben, die in der folgenden Tabelle aufgeführt werden, beispielsweise "VR". Dieser ACE ermöglicht das Anzeigen und Lesen von Objekten. Andere Zugriffsarten werden verweigert.

Ein leerer ACE (kein Codebuchstabe) bedeutet, dass keine Zugriffsrechte zugewiesen wurden.

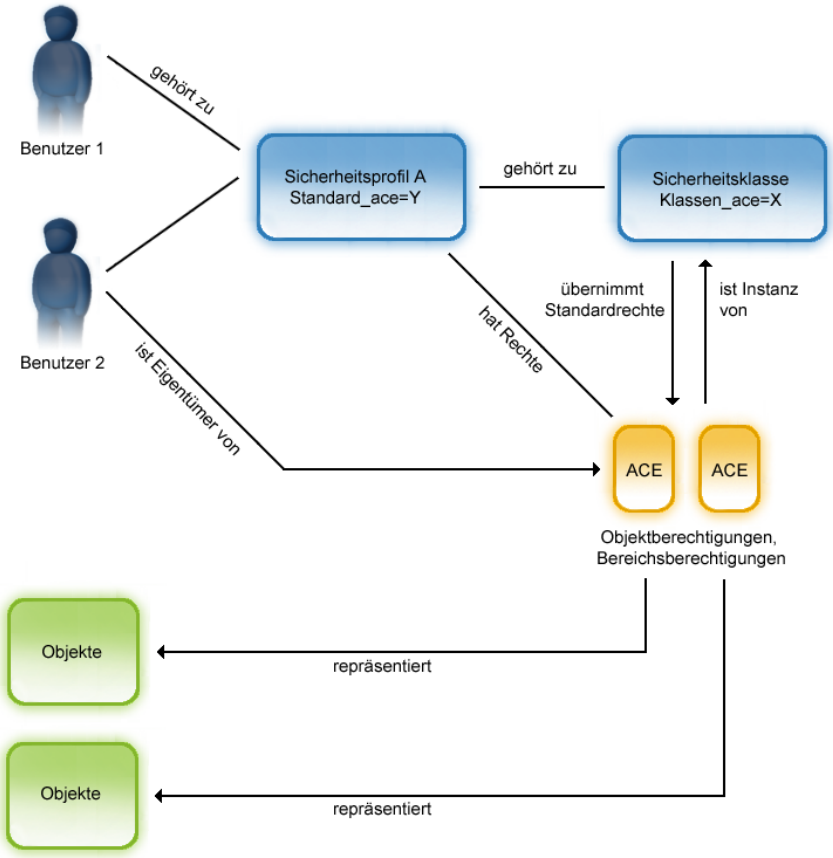
In der folgenden Tabelle sind Objektberechtigungen definiert:

Kennbuchstabe in ACE	Bedeutung	Gewährte Rechte
V	Ansicht	Damit können Sie Objekte anzeigen.

Kennbuchstabe in ACE	Bedeutung	Gewährte Rechte
V	Ansicht	Damit können Sie Objekte anzeigen.
C	Erstellen	Damit können Sie Objekte erstellen.
R	Gelesen	Damit können Sie die Unterobjekte eines Objekts lesen.
W	Schreiben	Damit können Sie ein Objekt ändern.
X	Ausführen	Damit können Sie abhängig vom Objekt ausführen.
D	Löschen	Damit können Sie Objekte löschen.
P	Berechtigung	Damit können Sie den ACE selbst ändern.
O	Ownership	Damit können Sie ein Objekt als Eigentum übernehmen.

Ein Benutzer kann einem oder mehreren Sicherheitsprofilen zugewiesen sein. Ein Benutzer kann auch Eigentümer eines Objektes sein. Jedem Sicherheitsprofil ist eine Gruppe von Sicherheitsklassen zugewiesen. Über die Sicherheitsklassenberechtigung wird die Standardberechtigung definiert, die einem Objekt zugewiesen wird, wenn eine Instanz der Klasse erstellt wird.

Die folgende Abbildung zeigt, wie Sicherheitsprofile, Sicherheitsklassen und Objektberechtigungen zusammenhängen und dass die Berechtigungen eines Objekts von der Sicherheitsklasse übernommen werden, deren Instanz es ist.



In der Abbildung gehört Benutzer 1 zum Sicherheitsprofil A. Benutzer 2 gehört zum Sicherheitsprofil A und ist Eigentümer der Objekte, dargestellt durch einen ACE. Benutzer 1 und Benutzer 2 haben bestimmte ACEs, z. B. VR, durch das Sicherheitsprofil A. Benutzer 2 hat einen zusätzlichen ACE, z. B. VCRWD, als Eigentümer eines Objekts.

Um die Zugriffsrechte von Benutzer 1 und Benutzer 2 zu prüfen, vereinigt das Sicherheitssystem den benutzerspezifischen ACE und den mit dem bestimmten gesicherten Objekt verknüpften ACE (logisch). In diesem Beispiel haben Benutzer 1 und 2 Anzeige- und Leserechte für das Objekt. Jedoch verfügt nur Benutzer 2 über Schreib- und Löschzugriff.

Sicherheitsebenen

Es gibt unterschiedliche Typen von Sicherheitsebenen für Objekte, die von der Art der Ableitung der Objektberechtigungen abhängen:

Sicherheit auf Klassenebene

Wenn die Objektberechtigung von der Berechtigung auf Klassenebene (von der Klasse, zu der das Objekt gehört) abgeleitet wird, ist die Sicherheit auf Klassenebene aktiviert. Dies ist die Standardeinstellung, wenn ein gesichertes Objekt erstellt wird.

Sicherheit auf Gruppenebene

Wenn ein gesichertes Objekt Mitglied einer Sicherheitsgruppe ist, für die die Übernahme aktiviert ist, ist die Sicherheit auf Gruppenebene aktiviert. Berechtigungen werden von der Gruppe abgeleitet, zu der das Objekt gehört (Berechtigung auf Gruppenebene).

Sicherheit auf Objektebene

Wenn der Benutzer die Objektberechtigung für ein bestimmtes gesichertes Objekt manuell einstellt, ist als Sicherheitsebene die Objektebene eingestellt, da die Berechtigungen individuell für das Objekt festgelegt werden.

Übernahme der Berechtigung aus einer Gruppe

Wenn ein Objekt Mitglied einer Gruppe ist, unterstützt das Sicherheitsuntersystem von CA ITCM die dynamische Übernahme von Gruppen an Mitglieder wie folgt:

- Ein Flag markiert eine Gruppe für die dynamische Übernahme.
- Die angegebenen Berechtigungen der Mitglieder werden von allen Mitgliedern dieser Gruppe übernommen.
- Wenn der Gruppe ein Mitglied hinzugefügt wird, übernimmt es automatisch die Berechtigungen der Gruppe.

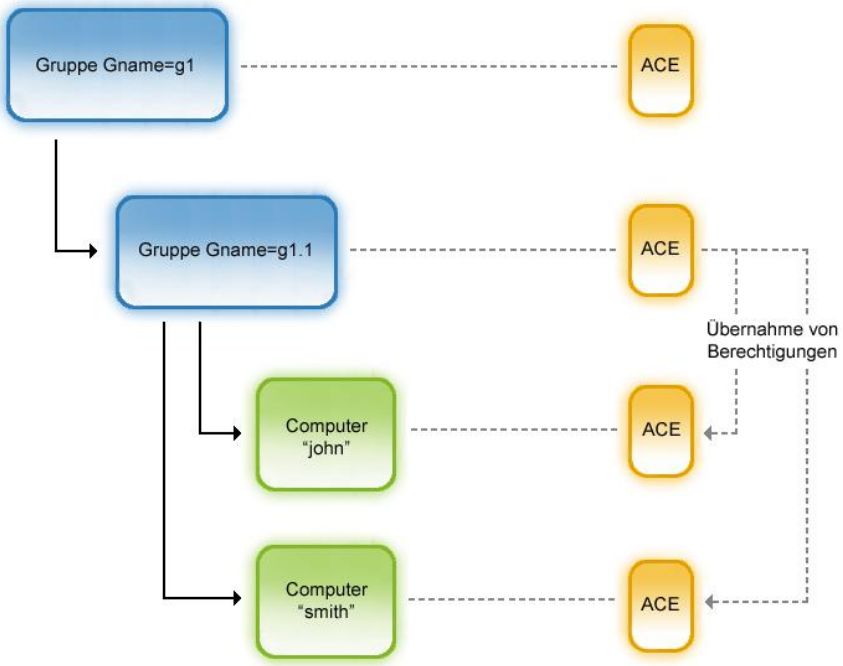
Das Modell der Gruppensicherheit basiert auf folgenden Entscheidungen:

- Die Übernahme der Sicherheit kann für eine Gruppe aktiviert oder deaktiviert werden. Wenn sie aktiviert ist, wird die Gruppe zu einer Sicherheitsgruppe. (In der Anwendung kann ein anderes Symbol für die Darstellung verwendet werden.)
- Die Gruppe verfügt über zwei Berechtigungsmasken, eine für die Gruppe selbst (wie alle anderen gesicherten Objekte) und eine Übernahmemaske.
- Wenn eine Gruppe Berechtigungen von einer übergeordneten Gruppe übernimmt, werden beide Masken in die Übernahmemaske der übergeordneten Gruppe geändert.

- Die Berechtigungsmaske eines Mitglieds einer oder mehrerer Gruppen wird entsprechend der "Vereinigungsmenge" aller Berechtigungen der übergeordneten Elemente des Mitgliedes evaluiert usw. (OR-Verknüpfung der Berechtigungen).
- Da untergeordnete Elemente Berechtigungen von übergeordneten Elementen übernehmen, kann es zu einer rekursiven Aktualisierung von Objekten kommen.
- Die Anzahl der Ebenen für die Übernahme ist nicht beschränkt.
- Objektberechtigungen haben gemäß den Vorrangregeln Vorrang vor Gruppenberechtigungen, diese wiederum haben Vorrang vor Klassenberechtigungen.
- Ist ein Objekt Mitglied mindestens einer Sicherheitsgruppe, darf dieses mit Ausnahme der Anwendung der Objektsicherheit nicht geändert werden, da die Anwendung der Klassensicherheit einen Fehler im Modell verursachen würde. Um die Klassensicherheit zu aktivieren, muss das Objekt aus der Gruppe entfernt werden, oder die Übernahme der Sicherheit muss für die Gruppe deaktiviert werden.

Hinweis: Die Übernahme der Berechtigung aus einer Gruppe wird deaktiviert, wenn als Sicherheitsebene eines Objekts die Objektebene festgelegt ist.

Die folgende Abbildung veranschaulicht die Übernahme, wenn ein Objekt Mitglied einer Gruppe ist und die Gruppe die Übernahme der Objektberechtigung zulässt:



Gruppe g1.1 ist eine Untergruppe von Gruppe g1. Die Computer "john" und "smith" sind Mitglieder der Gruppe g1.1.

Für die Gruppe g1 ist die Übernahme von Berechtigungen deaktiviert, für Gruppe g1.1 jedoch aktiviert. Daher übernehmen die Computer "john" und "smith" als Berechtigungen die Berechtigungen der Gruppe g1.1.

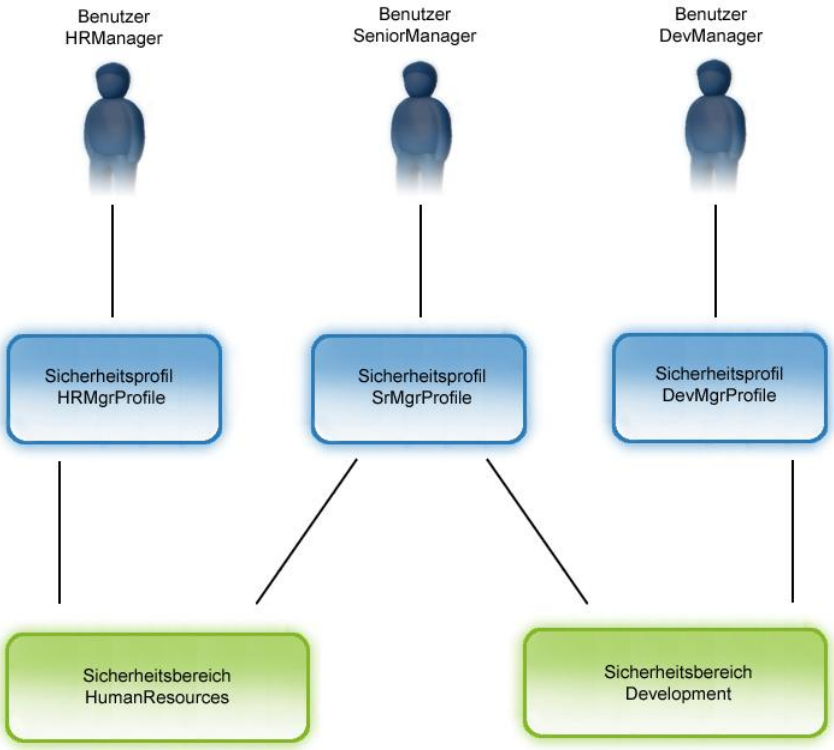
Bereichsberechtigungen

Das Konzept der Sicherheitsbereiche ist eine Ergänzung des Sicherheitsmodells. Ein Sicherheitsbereich ist eine optionale Funktion, die für umfangreiche Implementierungen mit Tausenden von Objekten, die von verschiedenen Benutzern verwaltet werden, geeignet ist.

Bei einem Sicherheitsbereich handelt es sich um einen geografischen oder topologischen Bereich oder einen Organisationsbereich. Das Definieren von Sicherheitsbereichen ist sinnvoll, wenn Sie den Zugriff der Benutzer auf die mit ihrem Sicherheitsbereich verknüpften Objekte beschränken möchten. Im Konzept der Sicherheitsbereiche werden Benutzer, die durch Sicherheitsprofile und Objekte dargestellt werden, mit Sicherheitsbereichen verknüpft. Ein Sicherheitsbereich kann mit einem oder mehreren Profilen und Objekten verknüpft werden. Ein Benutzer kann auf ein Objekt zugreifen, wenn mindestens ein mit dem Objekt verknüpfter Sicherheitsbereich auch mit mindestens einem Sicherheitsprofil des Benutzers verknüpft ist. Wird der Zugriff auf das Objekt verweigert, wird es dem Benutzer nicht angezeigt.

Beispiel: Zwei Sicherheitsbereiche und drei Benutzer

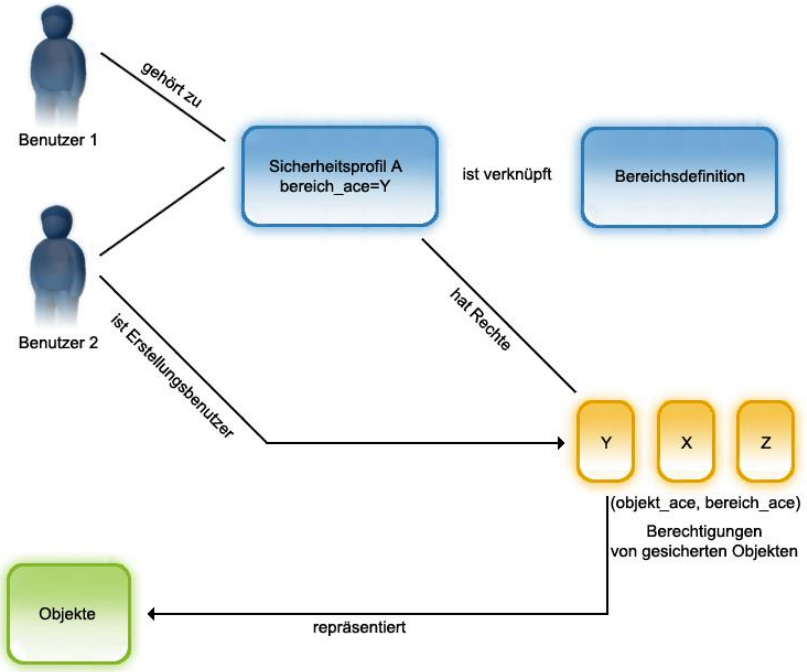
Den drei Benutzern HRManager, SeniorManager und DevManager sind die Benutzerprofile HRMgrProfile, SrMgrProfile und DevMgrProfile (mit allen Zugriffsrechten) zugewiesen. Zwei Sicherheitsbereiche, HumanResources und Development, wurden definiert. Die Profile HRMgrProfile und SrMgrProfile sind mit dem Sicherheitsbereich HumanResources verknüpft. Die Profile SrMgrProfile und DevMgrProfile sind mit dem Sicherheitsbereich Development verknüpft. Dann hat SeniorManager, repräsentiert von SrMgrProfile, Zugriff auf die beiden Sicherheitsbereiche HumanResources und Development. HRManager hat lediglich Zugriffsrechte für den Sicherheitsbereich HumanResources und DevManager lediglich für den Sicherheitsbereich Development. Wenn HRManager beispielsweise auf seiner Konsole eine Abfrage im Bereich HumanResources erstellt, wird dies DevManager nicht angezeigt. Nur vom System erstellte Objekte werden allen Benutzerprofilen angezeigt.



Durch Festlegen von Bereichsberechtigungen kann der Zugriff auf ein bestimmtes Objekt für ein oder mehrere Profile beschränkt werden. Dies bedeutet, dass selbst die für ein Profil festgelegten Berechtigungen auf Klassenebene übereinstimmen. Sie können ein Objekt verschiedenen Bereichen zuweisen oder es mit ihnen verknüpfen. Sie können den Zugriff auf Profile auch einschränken, so dass nur Objekte angezeigt werden, die mit einem bestimmten Bereich verknüpft sind.

Neben den Objektberechtigungen, die hauptsächlich über die Sicherheitsklassen verwaltet werden, können Sie im Sicherheitsuntersystem bis zu 32 Bereiche erstellen.

Die folgende Abbildung bietet eine Übersicht über die Bereichsunterstützung des Sicherheitsuntersystems.



Benutzer 1 und Benutzer 2 gehören zu Sicherheitsprofil "A". In der Bereichsdefinition, die mit Profil "A" verknüpft ist, wurden die Bereiche festgelegt, die den Benutzern angezeigt werden, die zum Sicherheitsprofil "A" gehören.

Benutzer 2 hat ein Objekt erstellt, das allen Benutzern angezeigt wird, die mit dem entsprechenden Bereich verknüpft sind.

Wichtige Verwendungsbeispiele und Erläuterungen der entsprechenden Funktionsweise der Bereichsunterstützung finden Sie im Abschnitt "Verwendungsbeispiele für die Unterstützung von Sicherheitsbereichen (siehe Seite 585)".

Vorbedingungen für Objektzugriff in Bereichen

Die folgenden Bedingungen müssen erfüllt sein, damit die Bereichsberechtigung des Benutzers evaluiert werden kann:

- Der Benutzer muss über Objektzugriff auf das Objekt verfügen (Berechtigung zum Anzeigen oder Lesen).
- Die Unterstützung der Sicherheitsbereiche muss auf dem Domänen-Manager aktiviert sein.
- Alle Sicherheitsprofile, deren Mitglied der Benutzer ist, müssen für die Unterstützung der Sicherheitsbereiche aktiviert sein.

Wenn die erste Bedingung nicht erfüllt ist, wird der Zugriff des Benutzers auf das Objekt verweigert, und zwar unabhängig davon, ob die zweite und dritte Bedingung erfüllt sind. Ist die zweite oder dritte Bedingung nicht erfüllt, unterliegt der Benutzer basierend auf den Bereichsberechtigungen keinen Einschränkungen, und er kann auf alle Objekte zugreifen.

Hinweise:

- Alle Benutzer, die Mitglied von Sicherheitsprofilen mit deaktiviertem Sicherheitsbereich sind, können auf alle Objekte zugreifen. Der Administrator sollte sicherstellen, dass alle Sicherheitsprofile für die Unterstützung der Sicherheitsbereiche aktiviert sind.
- Auf DSM-Enterprise-Managern werden Sicherheitsbereiche nicht unterstützt.
- Das einzige integrierte Profil, das für die Unterstützung der Sicherheitsbereiche aktiviert werden kann, ist das Profil "Verteilungen". Alle anderen integrierten Profile sind für die Unterstützung der Sicherheitsbereiche deaktiviert.
- Objekte, die zu den Sicherheitsklassen "Prozedur" und "Softwarejob" gehören, können im DSM-Explorer mit keinem Sicherheitsbereich verknüpft werden. Sie werden automatisch mit den Bereichen der jeweiligen übergeordneten Container ("Softwarepaket" und "Softwarejobcontainer") verknüpft.

Abgeleitete Bereichsberechtigungen

Bereichsbedingungen können folgendermaßen festgelegt oder abgeleitet werden:

Bereichsberechtigung von Sicherheitsprofil

Wenn der Erstellungsbenutzer beim Erstellen eines gesicherten Objektes gültig ist, werden die Bereichsberechtigungen von dem Benutzer abgeleitet, der das Objekt erstellt.

(Sicherheitsebene: Erstellungsbenutzer)

Bereichsberechtigung von Gruppe

Dieser Fall tritt nur ein, wenn das gesicherte Objekt Mitglied einer Gruppe und die Übernahme aktiviert ist.

(Sicherheitsebene: Gruppe)

Manuell festgelegte Bereichsberechtigung

Benutzer können die Bereichsberechtigung für ein bestimmtes Objekt manuell festlegen.

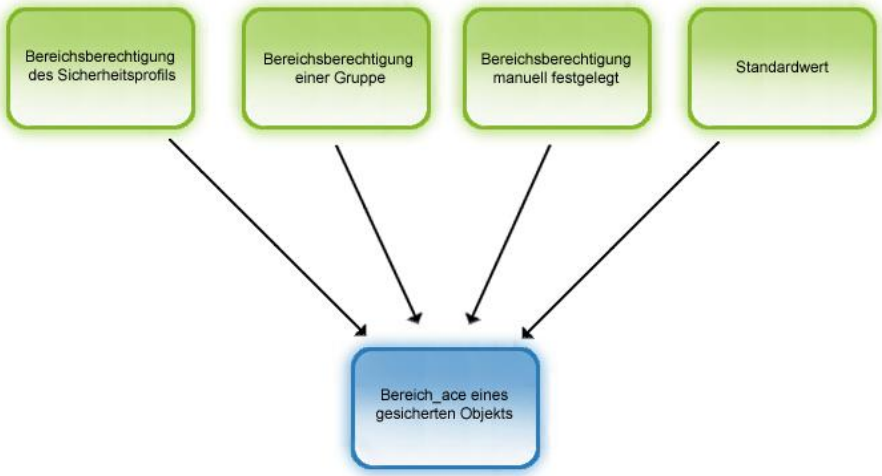
(Sicherheitsebene: Objekt)

Standard-Bereichsberechtigung

Wenn ein gesichertes Objekt erstellt wird und der Erstellungsbenutzer nicht angegeben wurde oder nicht in der Benutzerliste gefunden wird, werden die Bereichsberechtigungen von den globalen Konfigurationseinstellungen (globalen Standardberechtigungen) abgeleitet.

(Sicherheitsebene: Globale Einstellungen)

Die folgende Abbildung zeigt, auf welche Arten die Bereichsberechtigung eines Objekts abgeleitet werden kann:



Replikation

Bei der Replikation zwischen Enterprise und Domäne berücksichtigt das Sicherheitsuntersystem keine Autorisierungsdaten. Aufgrund der großen Anzahl von Objekten mit Berechtigungsdaten sind sie nicht für die Replikation geeignet. Stattdessen wird die Sicherheit für Objekte, die von einer Datenbank an eine andere übertragen werden, zurückgesetzt.

D. h. die Berechtigungen (Objekt- und Bereichsberechtigungen) werden neu berechnet, sobald ein repliziertes gesichertes Objekt erstellt wird. Dies gilt für beide Richtungen der Replikation. Die Replikation der Bereichsdefinitionen ist beispielsweise nicht erforderlich.

- **Vorbedingungen**
  - Von einem Benutzer X wird auf Enterprise-Ebene eine Abfrage erstellt.
  - Benutzer X hat nur Zugriff auf die Bereiche 1 und 2.
  - Benutzer X ist auch auf Domänenebene bekannt und hat nur Zugriff zu Bereich 5.
- **Aktion**

  Eine Abfrage wird abwärts repliziert.
- **Nachbedingungen**
  - Eine Abfrage wird auf Domänenebene erstellt.
  - Die Bereichsberechtigung wird als vom Erstellungsbenutzer definiert festgelegt, in diesem Fall für den Benutzer X.
  - Benutzer X wird die Abfrage auf Domänenebene nicht angezeigt, weil er keine Bereichsberechtigungen für die Bereiche 1 und 2 hat.

Einschränkungen

- Software Delivery-Tasks werden in der Systemsteuerung für alle Administratoren immer angezeigt, da die Tasks nicht gesichert sind (weder Objekte noch Bereichsberechtigungen). Die Task-Liste ist jedoch schreibgeschützt.
- Berechtigungen für Software Delivery-Anwendungsobjekte werden vom Zielobjekt abgeleitet.
- Die Anzahl der Bereiche ist auf 32 beschränkt.

Sicherheitsszenario – Software Delivery

Im folgenden Szenario werden die Grundlagen des Sicherheitskonzepts dargestellt.

Szenario:

Sie möchten einem Benutzer erlauben, Software zu erstellen und ihm vollständige Berechtigungen zum Bearbeiten und Verteilen dieser Software für eine bestimmte Computergruppe gewähren. Anderen Benutzern möchten Sie diese Berechtigungen nicht gewähren.

Sie können mehr als eine Benutzergruppe erstellen und damit unabhängige Inseln mit Unteradministratoren erhalten.

Öffnen Sie das Dialogfeld "Sicherheitsprofile". Nehmen Sie an den Gruppen "Jeder" und "Eigentümer/Ersteller" keine Änderungen vor. Sie können die Administratorgruppe für Benutzer mit weiteren umfassenden Berechtigungen reservieren. Daher sollten Sie für dieses Szenario einige neue Sicherheitsprofile definieren.

So implementieren Sie das oben genannte Szenario:

1. Erstellen Sie ein neues Sicherheitsprofil namens USER1 (Benutzerkonto), das für eine eingeschränkte Verwendung vorgesehen ist.
2. Stellen Sie über die Administratorengruppe die Klassenberechtigungen für dieses Profil wie in der folgenden Tabelle angegeben ein:

Objektklasse	Klassenberechtigungen	Kommentare
Softwarepaket	Spezieller Zugriff (C)	Erstellt das Softwarepaket. Es sind keine weiteren Rechte erforderlich, da Sie nach dem Erstellen des Pakets sein Eigentümer sind.
Prozedur	Spezieller Zugriff (C)	Erstellt eine Prozedur.
Softwarejob	Spezieller Zugriff (C)	Erstellt einen Softwarejob auf dem Zielcomputer:
Softwarejobcontainer	Spezieller Zugriff (CVRW)	Erstellt den Jobcontainer, schreibt in ihn und zeigt ihn an. Verfügbar im Ordner "Jobs", "Softwarejobs", "Alle Softwarejobs".

Objektklasse	Klassenberechtigungen	Kommentare
Softwarepaket	Spezieller Zugriff (C)	Erstellt das Softwarepaket. Es sind keine weiteren Rechte erforderlich, da Sie nach dem Erstellen des Pakets sein Eigentümer sind.
Alle anderen Objektklassen	Kein Zugriff	Schränkt den Zugriff des Benutzers auf andere Objekte ein.

3. Navigieren Sie zur Asset-Gruppe, in der Sie die Software verteilen möchten, und stellen Sie die Gruppenberechtigungen für dieses Profil folgendermaßen ein:
   - Objektzugriff: Verwalten (VRX)
   - Mitgliederzugriff: Verwalten (VRX)

   Hinweis: Bei der spezifischen Asset-Gruppe muss es sich um eine Sicherheitsgruppe mit der Option "Mitglieder übernehmen Berechtigungen" handeln.
4. Stellen Sie im Dialogfeld "Objektberechtigungen" für die Objekte "Domäne" (Knoten), "Computer und Benutzer" und "Softwarepaketbibliothek" Leseberechtigungen (VR) ein.

Vom Benutzer erstellte Jobs werden dem Benutzer angezeigt.

Erstellen Sie ein entsprechendes Sicherheitsprofil für USER2. USER2 hat keinen Zugriff auf Computer, Softwaregruppen und Jobs von USER1 und umgekehrt.

Wenn USER1 die Installationen auf den Computern unter "Speziell" anzeigen möchte, werden die angeforderten Installationen angezeigt. Hier, aber an keiner anderen Stelle, wird für USER1 auch die auf diesen Computern installierte Software Delivery-Software angezeigt.

Konfigurieren von Common Security

Das Konfigurieren der Sicherheitsfunktionen ist einer der entscheidenden Schritte nach der Installation, da hier das Gateway zum CA IT Client Manager-System festgelegt wird. Sie können ein Sicherheitsmodell wählen, das auf Ihr Unternehmen abgestimmt ist und das Sicherheitssystem entsprechend einrichten. Die Wahl des Sicherheitsmodells kann auf Basis folgender Faktoren geschehen:

- Einzelne Benutzer und Gruppen (lokal und in der Domäne), die auf das System zugreifen müssen.
- Der Typ des Zugriffs (etwas Lesen, Schreiben, Ausführen usw.), den die Benutzer und Gruppen benötigen.
- Die erforderliche Berechtigungsebene, z. B. Berechtigungen auf Klassen-, Gruppen-, Objekt- oder Bereichsebene.

Hinweis: Wenn ein Benutzer über zwei Profile verfügt und ein Profil seinem Benutzerkonto und das andere einer Gruppe zugeordnet ist, werden die Berechtigungen in beiden Profilen vereinigt. Diese Regel gilt auch, wenn ein Benutzer Mitglied mehrerer Gruppen ist, die als Sicherheitsprofile definiert sind.

In der Standardeinstellung erhalten die Mitglieder der Administratorengruppe vollständige Zugriffskontrolle. Wenn die Installation von CA IT Client Manager vollständig ist, kann sich somit jedes Mitglied der Administratorengruppe bei der DSM-Domäne anmelden und weitere Benutzer erstellen und Zugriffsrechte gewähren.

So richten Sie die Sicherheitsfunktionen ein:

Mit den folgenden Tasks richten Sie den sicherheitsgesteuerten Zugriff auf das System ein. Wenn Sie diese Tasks verstehen, ist es leichter, ein leistungsfähiges und effizientes Sicherheitssystem einzurichten.

- Fügen Sie dem System Sicherheitsprofile hinzu. Vordefinierte Profile werden standardmäßig im Sicherheitssystem hinzugefügt und können nicht entfernt werden.
- Geben Sie die Klassenberechtigungen für die Objektklassen an, die im Dialogfeld "Klassenberechtigungen" aufgeführt sind.

  Stellen Sie sicher, dass die Profile nicht die Zugriffsrechte für die Objektklassen "Sicherheitsprofile", "Sicherheitsbereiche" und "Klassenberechtigungen" ändern können. Öffnen Sie die Profile, und legen Sie als Zugriffstyp für Klassenberechtigungen für alle drei Objektklassen "Kein Zugriff" fest.

Zur weiteren Feinabstimmung des Sicherheitssystems gehen Sie folgendermaßen vor:

- Legen Sie den Gruppenzugriff oder Objektzugriff für jeden Ordner oder jedes im Explorer sichtbare Objekt fest.
- Über "Spezieller Zugriff" wählen Sie eine Kombination von Zugriffsberechtigungen aus: Anzeigen, Lesen, Schreiben, Löschen, Ausführen, "Berechtigungen ändern" und "Als Eigentum übernehmen".

Nicht nur Administratoren, sondern alle Benutzer des Betriebssystems mit einem gültigem Konto auf dem Domänen-Manager können jetzt eine Verbindung zum System herstellen. Der Zugriff auf die Funktionen des Systems wird über die internen Sicherheitsmechanismen gesteuert. Standardmäßig erhalten Administratoren und der Eigentümer Vollzugriff. Alle anderen Benutzer erhalten keinen Zugriff. Sie können die Zugriffsrechte jedoch durch Aktualisieren der Berechtigungen nach der Installation ändern.

Hinweis: Wenn Sie mit dem Enterprise-Server verbunden sind, müssen Sie beachten, dass Sie für den Zugriff auf die Sicherheitsfunktionen auf den untergeordneten Domänen-Managern über ein Konto mit ausreichenden Benutzerrechten oder Benutzergruppenrechten verfügen müssen. Wenn Sie mit einem Domänen-Manager verbunden sind, müssen Sie beachten, dass Sie über ein Konto mit ausreichenden Rechten verfügen müssen, um auf die Sicherheitsfunktionen des Enterprise-Managers zuzugreifen.

Sicherheitsprofile hinzufügen

Wenn Sie ein Sicherheitsprofil erstellen, wird ein neues Sicherheitsprofil einem Benutzerkonto oder einer Gruppe zugeordnet, die von den aktuellen Sicherheitsprovidern bereitgestellt werden. Sie können die Benutzer oder Gruppen auswählen, die auf das System zugreifen können, und sie einem Sicherheitsprofil hinzufügen.

So fügen Sie Sicherheitsprofile hinzu:

1. Wählen Sie im Menü "Sicherheit" die Option "Sicherheitsprofile" aus.

   Das Dialogfeld "Sicherheitsprofile" wird angezeigt.

   Hinweis: Zum Öffnen dieses Dialogfelds müssen Sie über ausreichende Zugriffsrechte verfügen, anderenfalls wird eine Fehlermeldung angezeigt. Administratoren haben standardmäßig diese Zugriffsrechte.

2. Klicken Sie auf "Hinzufügen".

   Das Dialogfeld "Sicherheitsprofile hinzufügen" wird angezeigt.

3. Wählen Sie in der Baumstruktur "Verfügbare Verzeichnisse" die Sicherheitsautorität aus, suchen Sie nach dem erforderlichen Sicherheitsprinzipal, und klicken Sie auf diesen.

   In den Feldern "Container-ID" und "Namen" werden jeweils die ausgewählte Sicherheitsautorität und der Sicherheitsprinzipal angezeigt.

4. Doppelklicken Sie in der Struktur auf einen Prinzipal, oder klicken Sie auf "Zu Liste hinzufügen".

   Die Sicherheitsprinzipale im Feld "Namen" werden der Liste der Sicherheitsprofile hinzugefügt.

   Um weitere Profile hinzuzufügen, wiederholen Sie die letzten beiden Schritte im Dialogfeld "Sicherheitsprofile hinzufügen".

5. Klicken Sie auf "OK".

   Das ausgewählte Benutzerkonto oder die Gruppe wird dem Sicherheitsprofil zugeordnet und das Dialogfeld "Klassenberechtigungen" angezeigt.

   Hinweis: Wenn Sie mehr als ein Sicherheitsprinzipal hinzugefügt haben, wird das Dialogfeld "Klassenberechtigungen" nicht angezeigt. Sie müssen im Dialogfeld "Sicherheitsprofile" das Profil auswählen und auf "Klassenberechtigungen" klicken.

6. Wählen Sie im Dialogfeld "Klassenberechtigungen" die Objektklasse aus, der Sie die Rechte zuweisen möchten.

   Hinweis: Sie können mehrere Objektklassen auswählen und für alle die Klassenberechtigungen angeben. Um eine fortlaufende Auswahl zu treffen, drücken Sie die UMSCHALT-Taste und klicken auf die Objekte. Um eine zufällige Auswahl zu treffen, drücken Sie die STRG-Taste und klicken dann auf die Objekte.

7. Wählen Sie die Berechtigung in der Dropdown-Liste "Klassenzugriff" aus, und klicken Sie auf "OK".

   Die entsprechenden Berechtigungen werden dem neuen Sicherheitsprofil zugewiesen.

Das Dialogfeld "Sicherheitsprofile hinzufügen" wird mit einer Liste der verfügbaren Sicherheitsautoritäten angezeigt: Windows NT-Domänen, UNIX-Authentifizierungsziele, externe Verzeichnisse, z. B. NDS und LDAP, und das Untersystem des X.509-Zertifikats.

Die Liste der verfügbaren Sicherheitsautoritäten wird auf dem Manager gespeichert. In einer Windows NT-Domänenumgebung berechnet der Manager-Knoten automatisch alle verfügbaren expliziten Vertrauensverhältnisse für Domänen. Diese werden zur Anzeige zurückgegeben, wenn die Liste der verfügbaren Sicherheitsautoritäten über das Dialogfeld "Sicherheitsprofile hinzufügen" angefordert wird.

In einigen Fällen ist es sinnvoll, beim Erstellen von Sicherheitsprofilen eine implizit vertrauenswürdige Domäne zu verwenden, also eine Domäne, die nicht in der Ergebnisliste der Berechnung enthalten ist. Dies ist möglich, da Sie über das Dialogfeld "Sicherheitsprofile" Autoritäten hinzufügen und entfernen können, jedoch nur innerhalb des Namespace von Windows NT (winnt).

Um eine implizit vertrauenswürdige Domäne hinzuzufügen, klicken Sie auf "Hinzufügen" und geben im daraufhin angezeigten Dialogfeld den Namen der Domäne ein. Nachdem Sie auf "OK" geklickt haben ,wird die Domäne der Liste der verfügbaren Autoritäten hinzugefügt. Um eine implizit vertrauenswürdige Domäne zu entfernen, markieren Sie die entsprechende Domäne, und klicken Sie auf "Entfernen".

Durch das Hinzufügen einer Domäne zur Liste der Autoritäten wird diese nicht zu einer vertrauenswürdigen Domäne, dies wird vom Betriebssystem erzwungen. Wenn nicht ohnehin ein Vertrauensverhältnis zwischen einer Domäne und dem Betriebssystem besteht, ist es nicht möglich, dieser Liste diese Domäne hinzuzufügen, um ein Vertrauensverhältnis zwischen der Domäne und dem Manager zu schaffen.

Vordefinierte Zugriffstypen

Zugriffstypen geben die Rechte für den Zugriff auf ein Objekt oder einen Ordner an. Folgende Werte sind für Zugriffstypen möglich:

Ansicht

Anzeigeberechtigungen (V)

Gelesen

Berechtigungen zum Anzeigen und Lesen (VR)

Verwalten

Berechtigungen zum Anzeigen, Lesen und Ausführen (VRX)

Ändern

Berechtigungen zum Anzeigen, Lesen, Ausführen und Löschen (VRWXD).

Vollzugriff

Berechtigungen zum Erstellen, Anzeigen, Lesen, Schreiben, Ausführen, Löschen, Ändern von Berechtigungen und "Als Eigentum übernehmen" (CVRWXDPO).

Spezieller Zugriff

Wenn eine andere Kombination aus Rechten gewährt werden soll, wählen Sie "Spezieller Zugriff" aus. Das Dialogfeld "Spezieller Zugriff" wird angezeigt, in dem alle Rechte dargestellt sind.

Kein Zugriff

Blockiert den Zugriff des Benutzers auf Objekte in der Objektklasse.

Hinweis: Weisen Sie diesen Wert nicht der Gruppe "Eigentümer/Ersteller" zu. Damit könnte der Zugriff auf die Anwendung vollständig blockiert werden.

Im folgenden Beispiel werden die Auswirkungen der verschiedenen Zugriffsrechte in der Objektklasse "Computer" dargestellt:

Klassenzugriff	Entsprechende Berechtigung
Ansicht	Zeigt alle Computer im Ordner "Alle Computer" an.
Gelesen	Hierüber können Sie die Eigenschaften der Computer anzeigen.
Verwalten	Hierüber können Sie auf einem Computer ein Softwarepaket bereitstellen oder einen Job ausführen.
Ändern	Hierüber können Sie einen Computer hinzufügen oder einen Computer löschen.
Vollzugriff	Hierüber erhalten Sie vollständige Kontrolle über die Computer.

Klassenberechtigungen angeben

Sie können die einem Sicherheitsprofil zugewiesenen Klassenberechtigungen ändern.

So geben Sie Klassenberechtigungen an:

1. Wählen Sie im Menü "Sicherheit" die Option "Sicherheitsprofile" aus.

   Das Dialogfeld "Sicherheitsprofile" wird angezeigt.

2. Wählen Sie das Sicherheitsprofil aus, dessen Klassenberechtigungen Sie ändern möchten, und klicken Sie auf "Klassenberechtigungen".

   Das Dialogfeld "Klassenberechtigungen" wird angezeigt.

3. Wählen Sie die Objektklasse aus, der Sie die Rechte zuweisen möchten.

   Hinweis: Sie können mehrere Objektklassen auswählen und für alle die Klassenberechtigungen angeben. Um eine fortlaufende Auswahl zu treffen, drücken Sie die UMSCHALT-Taste und klicken auf die Objekte. Um eine zufällige Auswahl zu treffen, drücken Sie die STRG-Taste und klicken dann auf die Objekte.

4. Wählen Sie die Klassenberechtigungen im Feld "Klassenzugriff" aus, und klicken Sie auf "OK".

   Die Mitglieder des ausgewählten Sicherheitsprofils können nun im angegebenen Umfang auf die Objektklasse zugreifen.

   Um unterschiedliche Kombinationen von Rechten anzugeben, wählen Sie in dieser Dropdown-Liste für den Objektzugriff die Option "Spezieller Zugriff" aus.

Objektberechtigungen angeben

Sie können die Objektberechtigungen für jedes Objekt angeben, z. B. einen Computer, einen Benutzer, einen Job usw. Ein Objekt erbt standardmäßig die Klassenberechtigungen seiner Objektklasse.

Hinweis: Objektberechtigungen haben Vorrang vor Klassen- und Gruppenberechtigungen.

So geben Sie Objektberechtigungen an:

1. Wählen Sie die Objekte aus, und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie aus dem Menü "Sicherheit" die Option "Berechtigungen" aus.
   - Klicken Sie mit der rechten Maustaste auf das Objekt, und wählen Sie im Kontextmenü "Berechtigungen" aus.

   Das Dialogfeld "Objektberechtigungen" wird angezeigt.

   Hinweis: Sie können mehrere Objektklassen auswählen und für alle die Klassenberechtigungen angeben. Um eine fortlaufende Auswahl zu treffen, drücken Sie die UMSCHALT-Taste und klicken auf die Objekte. Um eine zufällige Auswahl zu treffen, drücken Sie die STRG-Taste und klicken dann auf die Objekte.
2. Wählen Sie in der Dropdown-Liste "Objektzugriff" den benötigten Zugriffstyp aus, und klicken Sie auf "OK".

   Die Mitglieder des Profils erhalten Zugriff im Rahmen der ihnen zugewiesenen Rechte.

   Um unterschiedliche Kombinationen von Rechten anzugeben, wählen Sie in dieser Dropdown-Liste für den Objektzugriff die Option "Spezieller Zugriff" aus.

Gruppenberechtigungen angeben

Gruppenberechtigungen können für benutzerseitig erstellte Ordner angegeben werden.

Hinweis: Objektberechtigungen haben gemäß den Vorrangregeln Vorrang vor Gruppenberechtigungen, diese wiederum haben Vorrang vor Klassenberechtigungen. Dies bedeutet, dass durch Festlegen von Klassenberechtigungen keine einzeln angegebenen Objekt- und Gruppenmitgliederberechtigungen ersetzt werden.

So geben Sie Gruppenberechtigungen an:

1. Wählen Sie den Ordner aus, und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie aus dem Menü "Sicherheit" die Option "Berechtigungen" aus.
   - Klicken Sie mit der rechten Maustaste auf die Gruppe, und wählen Sie im Kontextmenü "Berechtigungen" aus.

   Im angezeigten Dialogfeld "Sicherheitsgruppenberechtigungen" können Sie die Berechtigungen auf Gruppenebene einstellen.
2. Wählen Sie ein Profil aus, und geben Sie den Objektzugriff und den Mitgliedszugriff an.

   Hinweis: Bei Auswahl von "Standard" werden die Mitgliederberechtigungen von den Klassenberechtigungen überschrieben.

   Die Mitglieder des Profils können nun im angegebenen Umfang auf den Ordner oder die Gruppe zugreifen.

   Um unterschiedliche Kombinationen von Rechten anzugeben, wählen Sie in dieser Dropdown-Liste für den Objektzugriff die Option "Spezieller Zugriff" aus.

Alle Berechtigungen

Für zugewiesene Sicherheitsprofile gelten fast immer alle Berechtigungen, wie in den folgenden Aussagen und Beispielen erläutert wird:

- Wenn ein Benutzer mehreren Sicherheitsgruppen angehört, werden die Rechte aller Gruppen über die OR-Verknüpfung miteinander verbunden, um die Zugriffsrechte für den Benutzer festzulegen.

  Wenn ein Benutzer z. B. Mitglied in zwei Gruppen ist und eine Gruppe Schreibzugriff und die andere Lesezugriff auf ein Objekt hat, verfügt der Benutzer über Schreibzugriff.
- Berechtigungen auf Objektebene setzen Berechtigungen auf Gruppenebene außer Kraft, die wiederum Berechtigungen auf Klassenebene außer Kraft setzen.

Beispiele:

- Um einen Ordner zu erweitern, wenn Sie z. B. die Computer in einer Gruppe auflisten möchten, benötigen Sie Leserechte für diesen Ordner.
- Um ein Objekt zu erstellen, müssen Sie über Rechte zum Erstellen für das Objekt verfügen.

  Wenn das erstellte Objekt in einem Ordner abgelegt werden soll, müssen Sie auch über Lese- und Schreibrechte für diesen Ordner verfügen.
- Für die Vorgänge zum Einfügen und Verknüpfen sind Schreibrechte für den aktuellen Ordner oder das aktuelle Objekt erforderlich (wenn z. B. Dateien und Ordner eingefügt werden).
- Für den Verschiebevorgang sind sowohl für Quellordner oder Quellobjekte als auch für Zielordner oder Zielobjekte Schreibrechte erforderlich.

Unterstützung der Sicherheitsbereiche

Bei einem Sicherheitsbereich handelt es sich um einen geografischen oder topologischen Bereich oder einen Organisationsbereich. Ein Sicherheitsbereich kann mit einem oder mehreren Sicherheitsprofilen und Objekten verknüpft werden. Ein Benutzer kann auf ein Objekt zugreifen, wenn mindestens ein mit dem Objekt verknüpfter Sicherheitsbereich auch mit mindestens einem Sicherheitsprofil des Benutzers verknüpft ist.

Wichtige Verwendungsbeispiele und Erläuterungen der entsprechenden Funktionsweise der Bereichsunterstützung finden Sie im Abschnitt "Verwendungsbeispiele für die Unterstützung von Sicherheitsbereichen (siehe Seite 585)".

In den folgenden Abschnitten finden Sie Informationen zur Arbeit mit Sicherheitsbereichen.

Globale Einstellungen für Sicherheitsbereiche

Mit globalen Einstellungen wird neben dem Status der Unterstützung der Sicherheitsbereiche auch definiert, ob vom System erstellte Objekte im Sicherheitsbereich angezeigt werden. Sie können die globalen Einstellungen im Dialogfeld "Sicherheitsbereiche" ändern, das über das Menü "Sicherheit" aufgerufen werden kann.

Die Unterstützung der Sicherheitsbereiche ist auf dem Domänen-Manager standardmäßig deaktiviert. Sie müssen die Bereichsunterstützung aktivieren, um die Sicherheitsbereichfunktion in Ihrem Sicherheitssystem zu implementieren. Sie können jedoch auch Bereiche erstellen und mit Profilen und Objekten verknüpfen, ohne diese Option zu aktivieren. Um die Unterstützung für Sicherheitsbereiche auf dem Domänen-Manager zu aktivieren, aktivieren Sie im Feld "Unterstützung für Sicherheitsbereich" die Optionsschaltfläche "An".

Standardmäßig sind Sicherheitsbereiche so konfiguriert, dass vom System erstellte Objekte angezeigt werden. Wenn Sie vom System erstellte Objekte in einem bestimmten Sicherheitsbereich ausblenden möchten, deaktivieren Sie im Dialogfeld "Sicherheitsbereiche" das Kontrollkästchen neben dem Namen des Sicherheitsbereichs.

Aktivieren der Sicherheitsbereicheinstellung für ein Sicherheitsprofil

Sie müssen die Unterstützung der Sicherheitsbereiche für jedes geeignete Sicherheitsprofil aktivieren, um diese Funktion auf Sicherheitsprofilebene zu implementieren.

So aktivieren Sie die Sicherheitsbereicheinstellung für ein Sicherheitsprofil:

1. Wählen Sie im Menü "Sicherheit" die Option "Sicherheitsprofile" aus.

   Das Dialogfeld "Sicherheitsprofile" wird angezeigt.

2. Wählen Sie die Sicherheitsprofile aus, für die Sie die Sicherheitsbereicheinstellungen aktivieren möchten, und klicken Sie auf "Sicherheitsbereiche".

   Das Dialogfeld "Verknüpfungen der Sicherheitsbereiche" wird angezeigt.

3. Aktivieren Sie das Kontrollkästchen "Unterstützung von Sicherheitsbereichen für dieses Profil aktivieren".

   Auf dem Symbol neben dem Kontrollkästchen wird ein grünes Häkchen angezeigt, das angibt, dass die Unterstützung der Sicherheitsbereiche aktiviert ist.

Erstellen von Sicherheitsbereichen

Sie können Bereiche für jede geografische oder topologische Einheit, Organisationseinheit oder beliebige andere Verwaltungseinheiten erstellen.

So erstellen Sie Sicherheitsbereiche:

1. Wählen Sie im Menü "Sicherheit" die Option "Sicherheitsbereiche" aus.

   Das Dialogfeld "Sicherheitsbereiche" wird angezeigt.

2. Klicken Sie auf "Hinzufügen".

   Das Dialogfeld "Neuer Sicherheitsbereich" wird angezeigt.

3. Geben Sie einen Namen sowie eine Beschreibung für den neuen Bereich ein, und klicken Sie auf "OK".

   Der neue Bereich wird der Liste der Sicherheitsbereiche im Dialogfeld "Sicherheitsbereiche" hinzugefügt, und das Dialogfeld "Verknüpfungen der Sicherheitsprofile" wird angezeigt, in dem Sie die Sicherheitsprofile mit dem neuen Bereich verknüpfen können.

Löschen von Sicherheitsbereichen

Wenn ein Sicherheitsbereich nicht mehr benötigt wird, können Sie ihn löschen. Gelöschte Sicherheitsbereiche werden aus dem System entfernt. Ihre Verknüpfungen mit Profilen und Objekten werden automatisch aufgehoben.

So löschen Sie Sicherheitsbereiche:

1. Wählen Sie im Menü "Sicherheit" die Option "Sicherheitsbereiche" aus.

   Das Dialogfeld "Sicherheitsbereiche" wird angezeigt.

2. Klicken Sie auf "Löschen".

   Eine Sicherheitsabfrage wird angezeigt.

3. Klicken Sie auf "Ja".

   Der Sicherheitsbereich wird gelöscht.

Verknüpfen von Sicherheitsbereichen mit Sicherheitsprofilen und Aufheben von Verknüpfungen

Wenn Sie ein Sicherheitsprofil mit einem Sicherheitsbereich verknüpfen, können Benutzer oder Gruppen nur auf die Objekte zugreifen, die mit ihren Sicherheitsbereichen verknüpft sind. Sie können ein Sicherheitsprofil mit einem oder mehreren geeigneten Sicherheitsbereichen verknüpfen. Bei mehreren Bereichen haben die Benutzer Zugriff auf Objekte, die mit allen zugehörigen Sicherheitsbereichen verknüpft sind.

Sie können die Verknüpfung eines Sicherheitsbereichs aufheben, wenn der Benutzer diesem nicht mehr angehört.

So verknüpfen Sie Sicherheitsbereiche oder heben Sie Verknüpfungen auf:

1. Wählen Sie im Menü "Sicherheit" die Option "Sicherheitsprofile" aus.

   Das Dialogfeld "Sicherheitsprofile" wird angezeigt.

2. Wählen Sie die Sicherheitsprofile aus, und klicken Sie auf "Sicherheitsbereiche".

   Das Dialogfeld "Verknüpfungen der Sicherheitsbereiche" wird mit dem Verknüpfungsstatus der ausgewählten Profile angezeigt.

3. Wählen Sie die Sicherheitsbereiche aus, und klicken Sie auf "Verknüpfung" bzw. "Verknüpfung entfernen".

   Die ausgewählten Sicherheitsprofile werden mit den Sicherheitsbereichen verknüpft, oder ihre Verknüpfung wird aufgehoben.

Verknüpfen von Sicherheitsbereichen mit gesicherten Objekten und Aufheben von Verknüpfungen

Wenn Sie ein gesichertes Objekt mit einem Sicherheitsbereich verknüpfen, haben nur Benutzer, die zu diesem Bereich gehören, Zugriff auf das Objekt. Sie können ein gesichertes Objekt mit einem oder mehreren geeigneten Bereichen verknüpfen. Bei mehreren Bereichen steht das Objekt Benutzern zur Verfügung, die mit allen Sicherheitsbereichen verknüpft sind, zu denen das Objekt gehört.

Hinweis: Wenn Sie ein Objekt mit einer Gruppe verknüpfen bzw. die Verknüpfung aufheben, übernimmt das Objekt automatisch die Bereichsberechtigungen der Gruppe, unabhängig davon, ob für das Objekt Bereichsberechtigungen definiert sind. Wenn Sie die Bereichsberechtigungen der Objektebene beibehalten möchten, müssen Sie nach dem Verknüpfen des Objektes bzw. nach dem Aufheben der Verknüpfung die Bereichsberechtigungen überprüfen und ändern.

So verknüpfen Sie Sicherheitsbereiche oder heben Sie Verknüpfungen auf:

1. Wählen Sie die Objekte im Explorer aus, und klicken Sie mit der rechten Maustaste darauf.

   Das entsprechende Kontextmenü wird angezeigt.

2. Wählen Sie "Berechtigungen" aus.

   Das Dialogfeld "Objektberechtigungen" wird angezeigt.

3. Klicken Sie auf "Sicherheitsbereiche".

   Das Dialogfeld "Verknüpfungen der Sicherheitsbereiche" wird mit dem Verknüpfungsstatus der ausgewählten Objekte angezeigt.

4. Wählen Sie die Sicherheitsbereiche aus, und klicken Sie auf "Verknüpfung" bzw. "Verknüpfung entfernen".

   Die ausgewählten gesicherten Objekte werden mit den Sicherheitsbereichen verknüpft, oder ihre Verknüpfung wird aufgehoben.

Konfigurieren der Verschlüsselung

CA ITCM bietet Unterstützung für starke Verschlüsselungsalgorithmen (vor allem für den Advanced Encryption Standard (AES)) des Session Messaging-Untersystems und den damit verbundenen Komponenten.

Sie können die für die Kommunikation mit anderen Partnern verwendeten Algorithmen mit Hilfe der Verschlüsselungsrichtlinien konfigurieren. Diese Konfiguration gilt für die Kommunikation mit Hilfe von Session Messaging, der Funktion zur Speicherung und Weiterleitung von Software Delivery, Remote Control-Viewer/-Host, des DTS-Agenten und des Software Delivery-Servers für Dateiübertragungen ohne NOS.

Die verfügbaren Verschlüsselungsalgorithmen, die Auswahl des besten Algorithmus für die Kommunikation und die Kommunikation mit Partnern, die eine frühere Version als r11.2 verwenden, werden in den folgenden Abschnitten behandelt:

- Verschlüsselungsalgorithmen für die Kommunikation (siehe Seite 449)
- Auswählen des entsprechenden Verschlüsselungsalgorithmus (siehe Seite 450)
- Verschlüsselung in Umgebungen mit höchster Geheimhaltungsstufe (siehe Seite 451)
- Kommunikation mit älteren Versionen (siehe Seite 451)

Verschlüsselungsalgorithmen für die Kommunikation

Der für die Kommunikation verwendete Verschlüsselungsalgorithmus und die bevorzugte Reihenfolge sind in einer Verschlüsselungsrichtlinie, der Liste für Cipher-Voreinstellungen definiert.

Bei der Erstellung einer Kommunikation werden die definierten Algorithmen beider Kommunikationspartner berücksichtigt, und der geeignetste Matching-Algorithmus in der Liste wird für die folgende Sitzung ausgewählt. Um eine Kommunikationssitzung erstellen zu können, muss mindestens ein allgemeiner Algorithmus von beiden Kommunikationspartnern gemeinsam verwendet werden.

In der folgenden Liste werden die verfügbaren Verschlüsselungsalgorithmen angezeigt, die in aufsteigender Reihenfolge nach ihrer Stärke sortiert sind (d. h., AES-256 ist der stärkste Algorithmus):

Triple-DES (Data Encryption Standard)

Gibt einen 168 Bit langen symmetrischen Schlüssel gemäß dem Data Encryption Standard an.

AES-128 (Advanced Encryption Standard)

Gibt einen 128 Bit langen symmetrischen Schlüssel gemäß dem Advanced Encryption Standard an.

AES-192

Gibt einen 192 Bit langen symmetrischen Schlüssel gemäß dem Advanced Encryption Standard an.

AES-256

Gibt einen 256 Bit langen symmetrischen Schlüssel gemäß dem Advanced Encryption Standard an.

Auswahl des entsprechenden Verschlüsselungsalgorithmus

Jeder Kommunikationspartner hat eine Liste mit bevorzugten Ciphern, die in der Verschlüsselungsrichtlinie definiert sind. Der Cipher mit der höchsten Priorität befindet sich ganz oben auf der Liste. Die Listen beider Kommunikationspartner werden gemäß den folgenden Regeln verglichen und evaluiert:

- Die Cipher werden in jeder Liste der Reihe nach verglichen, und in der anderen Liste wird nach dem entsprechenden Cipher gesucht, bis eine Übereinstimmung gefunden wird oder die Liste endet.
- Wenn zwei übereinstimmende Cipher vorhanden sind, wird der stärkere für die anschließende Sitzung verwendet.
- Wenn ein übereinstimmender Cipher vorhanden ist, wird dieser für die anschließende Sitzung verwendet.
- Wenn kein übereinstimmender Cipher gefunden wird, ist eine Kommunikation nicht möglich.

Beispiel:

Die Cipher-Liste des Partners A enthält: Triple-DES, AES-192, AES-128. Die Cipher-Liste des Partners B enthält: AES-256, AES-128, Triple-DES, AES-192.

Das System führt folgende Schritte aus, um übereinstimmende Cipher zu identifizieren:

1. Die Liste des Partners A wird durchsucht:

   Der erste Eintrag, Triple-DES, wird in der Liste des Partners B gesucht.

   Eine Übereinstimmung wird gefunden. Triple-DES ist der erste übereinstimmende Cipher.

2. Die Liste des Partners B wird durchsucht:

   Der erste Eintrag, AES-256, wird in der Liste des Partners A gesucht.

   Es wird keine Übereinstimmung gefunden.

   Der zweite Eintrag, AES-128, wird in der Liste des Partners A gesucht.

   Eine Übereinstimmung wird gefunden. AES-128 ist der zweite übereinstimmende Cipher.

3. Das System hält den Algorithmus AES-128 für stärker und verwendet ihn anstelle des Triple-DES für die anschließende Sitzung.

Hinweis: Es werden nur die ersten zwei Übereinstimmungen berücksichtigt. Weitere Such- oder Vergleichaktionen werden in den zwei Cipher-Listen nicht durchgeführt.

Verschlüsselung in Umgebungen mit höchster Geheimhaltungsstufe

Für Kunden, die eine Verschlüsselung in einer Umgebung mit höchster Geheimhaltungsstufe benötigen, sollten Sie zunächst den Manager installieren und die Standardrichtlinie für die Cipher-Voreinstellungen so ändern, dass die Liste nur AES-256 enthält, und die Eigenschaft "DSM/common components/encryption/compatibility/pre_11_2" auf "False" setzen.

Sobald die Konfigurationsänderung für den Agenten auf dem Managersystem ausgeführt (also der Konfigurationsjob abgeschlossen) wurde, ist die Installation der Scalability-Server sicher.

Auf der Scalability-Serverebene müssen Sie mit den folgenden Befehlen überprüfen, ob die Cipher-Liste verbreitet wurde:

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences -pncipher0
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences -pncipher1
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences -pncipher2
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences –pncipher3
```

Cipher 0 muss AES-256 enthalten, die übrigen Ciphers müssen leer sein. Dies kann auf der Managerebene oder der Agentenebene erfolgen, um zu überprüfen, ob die Cipher-Konfiguration bereits empfangen wurde.

Jetzt ist es sicher, Agenten zu installieren, die auf diesen Server verweisen. Die Agenten verwenden von Anfang an die AES-256-Verschlüsselung zur Kommunikation.

Sobald die allgemeine Konfiguration an die Agenten übertragen wurde, befindet sich auch in deren Cipher-Liste nur AES-256. Wenn ein anderer Cipher zur Kommunikation verwendet wird, schlägt sie fehl.

Kommunikation mit älteren Versionen (Kompatibilitätsrichtlinie)

Für die Kommunikation mit Produkten vor Versionr 11.2 muss die Kompatibilitätsrichtlinie "pre_11_2" auf "True" (Wahr) gesetzt werden.

In der Standardkonfiguration ist dieser Richtlinienwert gesetzt.

Wenn in der gesamten Umgebung keine Produkte vor Version 11.2 mehr installiert sind, setzen Sie die Kompatibilitätsrichtlinie "pre_11_2" auf "False" (Falsch), um den Sitzungsaufbau zu verbessern.

FIPS-konforme Kryptographie

CA ITCM unterstützt FIPS-konforme Kryptographie in zwei Modi - "FIPS-bevorzugt" und "nur-FIPS". Sie können in den Modus "nur-FIPS" wechseln, wenn das Upgrade aller Komponenten in Ihrer Infrastruktur durchgeführt wurden oder sie im Modus "FIPS-bevorzugter" funktionieren. Sie können bei Bedarf auch auf den Modus "FIPS-bevorzugt" zurückgreifen.

Weitere Informationen:

FIPS 140-2-Support (siehe Seite 80)

Bevor Sie den FIPS-Modus ändern

Bevor Sie den FIPS-Modus Ihrer CA ITCM-Infrastruktur ändern, müssen Sie die praktischen Hinweise für den Betrieb in einem bestimmten FIPS-Modus verstehen. Dieser Abschnitt listet die Hinweise und Voraussetzungen auf, die Sie überprüfen müssen, bevor Sie den FIPS-Modus ändern.

Gemischte FIPS-Modi

Wenn Ihre CA ITCM-Infrastruktur in gemischten FIPS-Modi funktioniert, d. h. einige Komponenten sind im Modus "FIPS-bevorzugt" und andere im Modus "nur-FIPS", gelten die folgenden Einschränkungen:

- Einige der OSIM-Funktionen funktionieren möglicherweise nicht einwandfrei, wenn die folgenden Komponenten kommunizieren:
  - Domänen-Manager im Modus "FIPS-bevorzugt" mit einem Scalability-Server im Modus "nur-FIPS"
  - Enterprise-Manager im Modus "FIPS-bevorzugt" mit einem Domänen-Manager im Modus "nur-FIPS"
- Die Kommunikation zwischen den folgenden Komponenten schlägt fehl:
  - CA ITCM r12-Komponenten mit DSM-Komponenten im Modus "Nur-FIPS"

Die folgenden Hinweise gelten, wenn Sie einen Domänen-Manager mit einem Enterprise-Manager verbinden:

- Sie können nur "Nur-FIPS"-Domänen-Manager mit einem "Nur-FIPS"-Enterprise Manager verbinden.
- Wenn der FIPS-Modus des Domänen-Manager oder des Enterprise Manager "FIPS-bevorzugt (Bereit für Nur-FIPS)" oder "FIPS-bevorzugt (Konvertierung für Nur-FIPS erneut -ausführen)"ist, können Sie keine Verknüpfungsoperation ausführen.
- Wenn der Enterprise Manager im Modus "FIPS-bevorzugt" ist, können Sie "FIPS-bevorzugt" oder frühere Domänen-Manager mit ihm verknüpfen.

"FIPS-bevorzugt" mit Modus "Nur-FIPS"

Die folgenden Operationen oder Funktionen werden nicht unterstützt, nachdem Sie vom Modus "FIPS-bevorzugt" in "Nur-FIPS" gewechselt haben:

- PLAIN- und CACRYPT-Verschlüsselungsfilter für DTS
- ADT-Funktionalität von vertrauenswürdigen Übertragungen und DTS-Domänen
- DTS-Übertragung mit Multicast oder Broadcast an eine Gruppe von Computern, die sowohl im Modus "Nur-FIPS" als auch im früheren Modus ausgeführt werden
- Erstellen oder öffnen Sie mit Kennwort verschlüsselte DNA-Dateien
- Verwendung eines früheren BS und Boot-Images, für die noch kein Upgrade durchgeführt wurde. Informationen zum Upgrade von Images finden Sie im *BS-Installationsverwaltungs-Administrationshandbuch*.

Voraussetzungen

Sie müssen überprüfen, dass Sie Folgendes erledigt haben, bevor Sie den FIPS-Modus ändern:

- Wenn Sie das Upgrade eines Clusters durchführen, deaktivieren Sie automatischen Start von CA ITCM auf allen Knoten eines Clusters vor dem Upgrade. Sie können den Services aktivieren, nachdem die Aktualisierung für alle Knoten im Cluster durchgeführt wurde.
- Schließen Sie alle Instanzen von DSM-Explorer (lokal und Remote), Webkonsole und CLI Sitzungen, wenn Sie das Konvertierungshilfsprogramm ausführen; Öffnen Sie keine neuen Instanzen, bis die Ausführung des Konvertierungshilfsprogramms abgeschlossen ist.
- Prüfen Sie, dass alle Konfigurationsrichtlinien auf den Enterprise- und Domänen-Managern versiegelt wurden.

So wechseln Sie in "nur-FIPS"

Beim Wechsel in den Modus "nur-FIPS" ermöglicht die CA ITCM-Infrastruktur nur die <Verwendung von FIPS-kompatibler Kryptographie. Nach dem Wechsel in den Modus "Nur-FIPS" können die Komponenten nicht mehr mit r12-Komponenten kommunizieren.

Hinweis: Wir empfehlen, dass Sie den Modus "FIPS-bevorzugt" verwenden, bis Sie bereit sind, nur FIPS-kompatible Kryptographie zu verwenden.

Der folgende Prozess beschreibt die Schritte für die Umstellung Ihrer CA ITCM-Infrastruktur in dem Modus "nur-FIPS":

Hinweis: Die zu einem Enterprise Manager gehörenden Schritte gelten nur, wenn Sie einen CA ITCM-Enterprise-Manager in Ihrer Umgebung haben.

1. Überprüfen Sie, dass für alle DSM-Komponenten ein Upgrade nach Version 12.8 durchgeführt wurde.
2. Aktualisieren Sie alle BS- und Boot-Images in ein FIPS-kompatibles Format. Weitere Informationen zum Aktualisieren von Images finden Sie im *BS-Installationsverwaltung - Administrationshandbuch*.
3. Führen Sie das Konvertierungshilfsprogramm im Enterprise Manager aus. Das Hilfsprogramm konvertiert globale OSIM-Konfigurationsrichtlinien in ein FIPS-kompatibles Format und verteilt verwaltete Werte und Parameterdefinitionen an alle Domänen-Manager.
4. Überprüfen Sie das Ereignisprotokoll des Enterprise Manager, um zu prüfen, dass die Richtlinie erfolgreich bei allen Domänen-Managern reproduziert worden ist.
5. Führen Sie das Konvertierungshilfsprogramm auf den Domänen-Managern aus. Das Hilfsprogramm konvertiert lokale OSIM-Konfigurationsrichtlinien und verteilt verwaltete Werte an alle Komponenten der CA ITCM-Infrastruktur.
6. Ändern Sie die Standardkonfigurationsrichtlinie auf dem Enterprise Manager, und wechseln Sie in den "Nur-FIPS"-Modus.

   Hinweis: Es wird davon abgeraten, den FIPS-Modus durch benutzerdefinierte Konfigurationsrichtlinien zu ändern.
7. Überprüfen Sie das Ereignisprotokoll des Enterprise Manager, um zu prüfen, dass die Richtlinie erfolgreich bei allen Domänen-Managern reproduziert worden ist.
8. Wenn Sie keinen Enterprise Manager haben, ändern Sie die Standardkonfigurationsrichtlinie auf den Domänen-Managern, und wechseln Sie in den" Nur-FIPS"-Modus.

Hinweis: Sie müssen CAF neu starten, damit der FIPS-Modus in Kraft tritt.

Weitere Informationen:

Unterstützte FIPS-Modi (siehe Seite 81)
Ausführen des Konvertierungshilfsprogramms (siehe Seite 456)
Ändern Sie die Konfigurationsrichtlinie, um den FIPS-Modus zu ändern (siehe Seite 458)

So wechseln Sie in "FIPS-bevorzugt"

In seltenen Umständen ist es erforderlich, dass CA ITCM mit Komponenten kommuniziert, die nicht FIPS-kompatibel sind, einem früheren Agent zum Beispiel, nachdem Sie die Infrastruktur auf den Modus "nur-FIPS" umgestellt haben. Der "nur-FIPS"-Modus unterstützt Rückwärtskompatibilität nicht, Sie müssen es auf wieder "FIPS-bevorzugt" einstellen.

Der folgende Prozess beschreibt die Schritte für die Umstellung Ihrer Infrastruktur in dem Modus "FIPS-bevorzugt":

Hinweis: Die zu einem Enterprise Manager gehörenden Schritte gelten nur, wenn Sie einen CA ITCM-Enterprise-Manager in Ihrer Umgebung haben.

1. Ändern Sie die Standardkonfigurationsrichtlinie auf dem Enterprise Manager, und wechseln Sie in den "FIPS-bevorzugt"-Modus.

   Hinweis: Es wird davon abgeraten, den FIPS-Modus durch benutzerdefinierte Konfigurationsrichtlinien zu ändern.

2. Überprüfen Sie das Ereignisprotokoll des Enterprise Manager, um zu prüfen, dass die Richtlinie erfolgreich bei allen Domänen-Managern reproduziert worden ist.

3. Wenn Sie keinen Enterprise Manager haben, ändern Sie die Standardkonfigurationsrichtlinie auf den Domänen-Managern, und wechseln Sie in den "FIPS-bevorzugt"-Modus.

   Hinweis: Sie müssen CAF neu starten, damit der FIPS-Modus in Kraft tritt. Sie müssen CAF mindestens auf dem Enterprise- oder Domänen-Manager neu gestartet haben, bevor Sie das Konvertierungshilfsprogramm darauf ausführen; sonst wird die Ausführung des Konvertierungshilfsprogramms fehlschlagen.

4. Führen Sie das Konvertierungshilfsprogramm auf der Enterprise Manager aus, um globale OSIM-Parameter in ein rückwärtskompatibles Format zu konvertieren.

5. Überprüfen Sie das Ereignisprotokoll des Enterprise Manager, um zu prüfen, dass die Richtlinie erfolgreich bei allen Domänen-Managern reproduziert worden ist.

6. Führen Sie das Konvertierungshilfsprogramm auf den Domänen-Manager aus, um lokale OSIM-Parameter in ein rückwärtskompatibles Format zu konvertieren.

Weitere Informationen:

Unterstützte FIPS-Modi (siehe Seite 81)
Ausführen des Konvertierungshilfsprogramms (siehe Seite 456)
Ändern Sie die Konfigurationsrichtlinie, um den FIPS-Modus zu ändern (siehe Seite 458)

Ausführen des Konvertierungshilfsprogramms

Die Ausführung des Konvertierungshilfsprogramms konfiguriert DSM-Komponenten für die Verwendung des erforderlichen FIPS-Modus. Führen Sie dieses Hilfsprogramm in der folgenden Reihenfolge aus:

- Enterprise Manager (wenn vorhanden)
- Domänen-Manager

So führen Sie das Konvertierungshilfsprogramm aus:

1. Überprüfen Sie, dass alle Konfigurationsrichtlinien auf dem Manager versiegelt werden.
2. Öffnen Sie das Fenster "Befehlszeile" und navigieren Sie zum Ordner *ITCM_installpath*\bin.
3. Führen Sie folgenden Befehl aus:

   `dmscript dsm_fips_conv.dms` *`FIPS_Mode`*

   FIPS_Mode

   Gibt den FIPS-Modus an, in den Sie wechseln möchten. Gültige Werte sind "Nur-FIPS" und "FIPS-bevorzugt".

   Nachdem die Ausführung des Hilfsprogramms abgeschlossen wurde, gibt es eine Erfolgs- oder Fehlermeldung aus. Wenn Sie das Hilfsprogramm mit dem Parameter NUR-FIPS ausgeführt haben, verändert das Hilfsprogramm den FIPS-Modus des entsprechenden Managers je nach dem Erfolg oder Fehler der Hilfsprogrammausführung.

4. Öffnen Sie DSM-Explorer auf dem Manager, klicken Sie auf den Stammknoten und überprüfen Sie das Systemstatus-Portlet auf FIPS 140 hin.

   Die FIPS-140-Einstellung zeigt den FIPS-Modus des Managers an.

   - Wenn das Hilfsprogramm erfolgreich ausgeführt wurde, zeigt diese Einstellung "FIPS-bevorzugt (Bereit für Nur-FIPS)" an. Sie können damit fortfahren, die Konfigurationsrichtlinie zu ändern, um den FIPS-Modus zu ändern.
   - Wenn die Ausführung des Hilfsprogramm fehlgeschlagen ist, zeigt die Einstellung "FIPS-bevorzugt (Fehler beim Ausführen von dsm_fips_conv)" an. Der Manager funktioniert weiterhin in diesem Modus, bis das Konvertierungshilfsprogramm erfolgreich auf dem Manager ausgeführt wird.

   Hinweis: Wenn der Manager in einem dieser zwei Modi operiert, werden r12-Clients (DSM-Explorer, CLI usw.) daran gehindert, sich mit dem Manager zu verbinden.

5. Führen Sie die folgenden Schritte aus, wenn das Hilfsprogramm mit Fehlern oder Warnungen abgeschlossen hatte:

   a. Zeigen Sie die Protokolldatei osimfiputil.log im Ordner *ITCM_installpath*\bin an wenn das Skript mit Fehlern oder Warnungen abgeschlossen wurde. Weitere Informationen finden Sie auch im Ereignisprotokoll.

   b. Führen Sie Verbesserungsmaßnahmen aus, um die Fehler zu beheben und das Konvertierungshilfsprogramm erneut auszuführen.

      Die DSM-Komponenten sind konfiguriert, um den erforderlichen FIPS-Modus zu verwenden.

Beispiel: Befehl für die Ausführung des Konvertierungshilfsprogramms für den "nur-FIPS"-Modus:

```
dmscript dsm_fips_conv.dms FIPS_ONLY
```

Weitere Informationen:

So wechseln Sie in "nur-FIPS" (siehe Seite 454)
So wechseln Sie in "FIPS-bevorzugt" (siehe Seite 455)
Prüfen Sie den FIPS-Modus von DSM-Komponenten (siehe Seite 460)

Ändern Sie die Konfigurationsrichtlinie, um den FIPS-Modus zu ändern

Sie müssen die Richtlinien zu "FIPS-bevorzugt" in der Standardkonfigurationsrichtlinie ändern, um den FIPS-Modus Ihrer CA ITCM-Infrastruktur zu ändern. Diese Richtlinien bestimmen den FIPS-Modus, in den Sie wechseln möchten, und was zu tun ist, bevor man den FIPS-Modus wechselt.

Wenn Sie einen Enterprise Manager haben, führen Sie die folgenden Schritte auf dem Enterprise Manager aus. Die Richtlinienänderungen werden in diesem Fall automatisch an alle zugeordneten Domänen-Managern, Scalability-Server, und Agenten verbreitet. Wenn Sie keinen Enterprise Manager haben, führen Sie die folgenden Schritte auf allen Domänen-Managern aus.

Hinweis: Führen Sie diese Aufgabe nur aus, wenn der FIPS-Modus des Managers "FIPS-bevorzugt" (Bereit für Nur-FIPS)" ist.

So ändern Sie die Konfigurationsrichtlinie, um den FIPS-Modus zu ändern

1. Navigieren Sie zu "Systemsteuerung", "Konfigurationsrichtlinie," klicken Sie mit der rechten Maustaste auf "Standardkonfigurationsrichtlinie" und "Un-Seal".

   Die Versiegelung der Richtlinie wird aufgehoben und sie ist bereit für Aktualisierungen.

   Hinweis: Es wird davon abgeraten, den FIPS-Modus durch benutzerdefinierte Konfigurationsrichtlinien zu ändern.

2. Navigieren Sie nach DSM, Common Components, Sicherheit, FIPS 140-Einstellungen und ändern die folgenden Richtlinien:

   FIPS 140-Einstellung

   Definiert den FIPS-Compliance-Level. Ändern Sie diese Einstellung, um den FIPS-Modus anzugeben, in den Sie wechseln möchten.

   Aktion ändern

   Definiert die auszuführenden Aktionen, wenn die FIPS 140-Richtlinie geändert wird.

   Hinweis: Weitere Informationen zu den Werten für die Einstellungen dieser Richtlinie finden Sie in der *DSM Explorer-Hilfe*.

3. Versiegeln Sie die Richtlinie auf dem Manager. Weitere Informationen zur Versiegelung der Richtlinie finden Sie im Abschnitt "Konfigurationsrichtlinie" der *DSM-Explorer Hilfe*.

   Die Richtlinienänderungen werden an alle zugeordneten DSM-Komponenten verbreitet. Dieser Prozess erfordert je nach der Größe Ihrer CA ITCM-Infrastruktur einige Zeit.

4. Ändern Sie den FIPS-Modus der folgenden Komponenten manuell, da die Richtlinienänderungen nicht automatisch an diese Komponenten verbreitet werden:

   - Eigenständiger Remote Control-Agent
   - Nicht verwaltete DSM-Agenten auf dem Enterprise Manager

     Hinweis: Ein nicht verwalteter Agent ist jener, der nicht mit einem Domänen-Manager verbunden ist. Wenn Sie anschließend den nicht verwalteten Agenten mit einem Domänen-Manager verbinden, wird der FIPS-Modus des Agenten vom FIPS-Modus des Domänen-Managers aufgehoben.

   Um den FIPS-Modus manuell zu verändern, verwenden Sie den folgenden Befehl:

   ```
   ccnfcmda –cmd setparametervalue –ps /itrm/common/security/fips140 –pn installmode –v FIPS_MODE
   ```

   FIPS_MODE

   Legt den FIPS-Modus fest. Geben Sie 1 für den Modus "FIPS-bevorzugt" und 2 für den Modus "nur-FIPS" ein.

   Wenn der Befehl erfolgreich ausgeführt wird, wird der angegebene FIPS-Modus auf dem Agenten festgelegt.

   Hinweis: Eigenständige DSM-Explorer und DSM-Reporter benötigen keine spezifische Konfiguration, da der DSM-Agent immer mit der eigenständigen-Installation dieser beiden Komponenten installiert wird. Die Agenten erhalten in diesem Fall automatisch die Richtlinienaktualisierung vom Manager.

5. Führen Sie den folgenden Befehl auf allen DSM-Komponenten aus, wenn Sie die Standardeinstellung der Change-Aktionsrichtlinie nicht geändert haben oder wenn Sie sie auf "FIPS-Modus beim nächsten Neustart von ITCM wechseln" festgelegt haben:

   ```
   caf stop
   caf start
   ```

   Nachdem der CAF neu gestartet wurde, funktioniert der Manager im neuen FIPS-Modus.

6. Starten Sie alle Instanzen von DSM-Explorer, DSM-Reporter und Webkonsole neu.

   Der aktualisierte FIPS-Modus ist jetzt im GUI verfügbar.

7. Überprüfen Sie, ob der FIPS-Modus der Agenten und Manager in den erforderlichen FIPS-Modus geändert wurden.

   Die Überprüfung stellt sicher, dass der Wechsel erfolgreich war.

   Hinweis: Wenn das Konvertierungshilfsprogramm nicht erfolgreich ausgeführt wird, bleibt der FIPS-Modus des Managers "FIPS-bevorzugt" (Fehler beim Ausführen von dsm_fips_conv).

Weitere Informationen:

So wechseln Sie in "nur-FIPS" (siehe Seite 454)
So wechseln Sie in "FIPS-bevorzugt" (siehe Seite 455)
Prüfen Sie den FIPS-Modus von DSM-Komponenten (siehe Seite 460)
Szenarien Wenn Änderungen der FIPS-Richtlinie nicht in Kraft treten (siehe Seite 463)

Prüfen Sie den FIPS-Modus von DSM-Komponenten

Sie können den FIPS-Modus von DSM-Managern, Scalability-Servern und Agenten ansehen, um zu prüfen, ob die Änderung erfolgreich war. Der FIPS-Modus ist in Form von Inventardaten verfügbar.

So zeigen Sie den FIPS-Modus von DSM-Komponenten an

1. Klicken Sie im DSM-Explorer auf den Stammknoten.

   Das Portlet "Systemstatus" zeigt den FIPS-Modus des Managers an.

2. Navigieren Sie zu "Computer und Benutzer", "Alle Computer", *"Computername"*, "Inventar", "Systemstatus"

   Das Attribut "FIPS-Modus" im rechten Bereich zeigt den FIPS-Modus des ausgewählten Computers an.

Hinweis: Sie können auch FIPS-spezifische Abfragen und Berichte ausführen, um den FIPS-Modus mehrerer Agent-Computer und Manager anzuzeigen.

Weitere Informationen:

Vordefinierte Abfragen und Berichte zum FIPS-Modus (siehe Seite 461)

Vordefinierte Abfragen und Berichte zum FIPS-Modus

Die folgenden vordefinierten Abfragen und der Bericht ermöglicht Ihnen, den FIPS-Modus der DSM-Komponenten in Ihrer Infrastruktur anzuzeigen:

Abfragen

Assets, die im Modus "Nur-FIPS" ausgeführt werden

Assets, die im Modus "FIPS-bevorzugt" ausgeführt werden

Assets, die ohne FIPS-Support ausgeführt werden

Berichte

Alle Computer nach FIPS-Modus

Hinweis: Der FIPS-Modus von r11.x- oder r12-Agentencomputern, die mit einem Version 12.8-Manager verbunden sind (und die im Modus "FIPS-bevorzugt" arbeiten), wird als "KEINER" angegeben. Der FIPS-Modus von NRI-Agenten wird als "N/V" angegeben.

Konfigurieren Sie FIPS-Compliance für DSM-Webkomponenten

Sie müssen Ihre Webkonsole, Browser, und den Webserver konfigurieren, um sicherzustellen, dass die Kommunikation zwischen Webkomponenten und anderen DSM-Komponenten FIPS-konform ist.

So konfigurieren Sie FIPS-Compliance für die CA ITCM-Webkonsole

1. Konfigurieren Sie SSL zwischen den folgenden Komponenten:
   a. Client-Browser und CA ITCM-Webkonsole
   b. CA ITCM-Webkonsole und CA ITCM-Webservices

   Hinweis: Weitere Informationen zur Konfiguration von TLS 1.0 auf IIS finden Sie im grünen Papier mit dem Titel *Securing the Web Admin Console Communication Using SSL (Sicherung der Verwendung der Web Admin-Konsole mit SSL)*. Weitere Informationen zur Konfiguration von TLS 1.0 auf einem Apache-Webserver finden Sie in der Dokumentation des Apache-Webserver.
2. Konfigurieren Sie Ihren Browser für die Verwendung von TLS 1.0 für die Kommunikation. Weitere Informationen finden Sie in der Browser-Dokumentation.
3. Konfigurieren Sie SSL mit FIPS-Compliance auf Ihrem Webserver. Information finden Sie in der Dokumentation Ihres Webservers.

4. Ändern Sie die Einstellungen in der Datei "*Install_Path*\Web-Console\webapps\wac\WEB-INF\classes\com\ca\wac\config\WACConfig.properties folgendermaßen:

   ```
   AMS_URL=https://Hostname/AMS/login.do
   WEBSERVICE_URL=https://Hostname/UDSM_R11_WebService/mod_gsoap.dll (Für Windows)
   WEBSERVICE_URL=https://Hostname/UDSM_R11_WebService (Für Linux)
   SSL_Enabled=True
   TrustStoreFileFullPath=truststorepath
   TrustStorePassword=Kennwort
   ```

   Die Webkonsole wird für die Verwendung von TLS für die gesamte Kommunikation konfiguriert.

5. Starten Sie tomcat mit den folgenden Befehlen neu:

   ```
   caf stop tomcat
   caf start tomcat
   ```

   Die aktualisierten Konfigurationen treten nach erfolgreichem Neustart von Tomcat in Kraft.

Reparieren eines mit einer r12-Komponente verbundenen Agenten vom Typ "Nur-FIPS"

Wenn ein Agent vom Typ "Nur-FIPS" mit einem r12-Manager oder Scalability-Server verbunden ist, können sie aufgrund inkompatibler FIPS-Modi nicht miteinander kommunizieren. Sie müssen entweder ein Upgrade des Managers oder des Scalability-Servers durchführen oder den FIPS-Modus des Agenten auf "FIPS-bevorzugt" festlegen.

So ändern Sie den FIPS-Modus des Agenten in "FIPS-bevorzugt"

1. Führen Sie den folgenden Befehl am Agent aus:

   ```
   ccnfcmda –cmd setparametervalue –ps /itrm/common/security/fips140 –pn installmode –v 1
   ```

   Wenn der Befehl erfolgreich ausgeführt wird, wird der FIPS-Modus auf dem Agenten als "FIPS-bevorzugt" festgelegt.

2. Starten Sie CAF mit den folgenden Befehlen neu:

   ```
   caf stop
   caf start
   ```

   Wenn CAF erfolgreich neu startet, operiert der Agent im Modus "FIPS-bevorzugt".

Szenarien Wenn Änderungen der FIPS-Richtlinie nicht in Kraft treten

Nachdem Sie die in der Konfigurationsrichtlinie festgelegte FIPS 140-Einstellung verändert und die Richtlinie auf dem Manager angewendet haben, führt CA ITCM die in der Change-Aktionsrichtlinie für diesen Wertset festgelegte Aktion aus. In den folgenden Szenarien treten die Änderungen der FIPS-Richtlinie nicht in Kraft und Sie sehen keine auf der Change-Aktionsrichtlinie basierende Aktion.

- Die Richtlinie ist noch nicht auf dem Zielcomputer eingetroffen - Überprüfen Sie die Einstellungen des Zielcomputers mit dem folgenden Befehl:

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn policy
  ```

  Der Befehl gibt 0 (frühere), 1 (FIPS-bevorzugt), oder 2 (Nur-FIPS) aus. Wenn der Befehl den neuen Wert für den FIPS-Modus zurückgibt, wird der neue Modus wirksam, wenn CA ITCM neu startet und den Wert in den Installmode-Parameter kopiert. Wenn der Befehl den neuen Wert für den FIPS-Modus nicht zurückgibt, zeigt es an, dass die Richtlinie noch nicht am Zielcomputer eingetroffen ist.

  Um den derzeitigen FIPS-Modus auf dem Zielcomputer zu erhalten, verwenden Sie den folgenden Befehl:

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn
  installmode
  ```

  Der Installmode-Parameter und der Richtlinienparameter müssen typischerweise den gleichen Wert enthalten. Wenn CA ITCM nicht neu gestartet worden ist, nachdem die Richtlinie angewandt wurde, wird der Installmode-Parameter allerdings weiter den vorherigen Richtlinienwert beibehalten, bis Sie CA ITCM neu starten.

  Hinweis: Für ausführlichere Information über den Ccnfcmda-Befehl zur Agentenkonfiguration tippen Sie "<command> /?" in der Befehlszeile eingeben.

- Eine "Nur-FIPS"-Richtlinie wird auf einen DSM-Manager angewendet, der entweder das Konvertierungshilfsprogramm nicht ausgeführt oder das Konvertierungshilfsprogramm mit Fehlern ausgeführt hat. Da der Modus "Nur-FIPS" erfordert, dass das Konvertierungshilfsprogramm erfolgreich ausgeführt wird, hat die Änderung der Richtlinie keine Wirkung, bis Sie das Konvertierungshilfsprogramm erfolgreich auf dem Manager ausführen:

  Um zu sehen, ob das Konvertierungshilfsprogramm auf dem Manager ausgeführt worden ist, verwenden Sie den folgenden Befehl:

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn
  ready_for_fips_only
  ```

  Wenn der Befehl 1 zurückgibt, zeigt es an, dass das Hilfsprogramm erfolgreich auf dem Manager ausgeführt worden ist.

  Hinweis: Das Konvertierungshilfsprogramm muss erfolgreich ausgeführt worden sein, wenn Sie versuchen, vom Modus "FIPS-bevorzugt" in den Modus "Nur-FIPS" oder aus dem Modus "Nur-FIPS" in den Modus "FIPS-bevorzugt" zu wechseln.

- Der neue FIPS-Modus ist der gleiche wie der derzeitige FIPS-Modus. Wenn der Zielcomputer schon im gleichen FIPS-Modus wie der neue FIPS-Modus funktioniert, treten die Änderungen nicht auf dem Zielcomputer in Kraft.
- Wenn die Change-Aktionsrichtlinie auf "Den Benutzer bitten, ITCM bei Bereitschaft neu zu starten" festgelegt wird, erscheint ein Dialogfeld, das den Benutzer auffordert, CA ITCM neu zu starten, wenn die Richtlinie den Zielcomputer erreicht. Wenn dieser Dialog nicht erscheint, überprüfen Sie den Parameter "restartaction" auf dem Zielcomputer mit dem folgenden Befehl:

  ```
  ccnfcmda –cmd getparametervalue –ps /itrm/common/security/fips140 –pn
  restartaction
  ```

  Wenn der Befehl nicht 2 zurückgibt, zeigt es an, dass die Richtlinie noch nicht beim Zielcomputer eingetroffen ist.

  Wichtig! Aktivieren Sie *nicht* die Option "Den Benutzer bitten, ITCM bei Bereitschaft neu zu starten" auf einem terminalen Server , da sonst alle Benutzern aufgefordert werden, CA ITCM neu zu starten!

Kapitel 12: ENC (Extended Network Connectivity)

Dieses Kapitel enthält folgende Themen:

Einführung in Extended Network Connectivity (siehe Seite 465)
ENC-Komponenten (siehe Seite 467)
Unterstützte Plattformen (siehe Seite 467)
ENC-Gateway-Verbindungsprozess (siehe Seite 468)
ENC-Gateway-Sicherheit (siehe Seite 469)
Authentifizierung (siehe Seite 469)
ENC-Gateway-Autorisierungsregeln (siehe Seite 470)
Auditing von Ereignissen (siehe Seite 488)
Installation und Konfiguration von ENC-Gateway-Komponenten (siehe Seite 489)
ENC- und SSA-Konfiguration (siehe Seite 489)
Aktivieren des ENC-Clients (siehe Seite 490)
Bereitstellung in einer ENC-Umgebung (siehe Seite 490)
ENC-Bereitstellungsszenarios (siehe Seite 491)
Internet-Proxy-Unterstützung (siehe Seite 504)
Einschränkungen für die Verwendung von CA ITCM über ein ENC-Gateway (siehe Seite 505)
Verwenden des Hilfsprogramms "encUtilCmd" (siehe Seite 507)
Verwaltung von Zertifikaten (siehe Seite 508)

Einführung in Extended Network Connectivity

CA IT Client Manager (CA ITCM) bietet die Gateway-Funktion "Extended Network Connectivity" (ENC), damit DSM-Komponenten und -Dienste Verbindungen zwischen Endpunkten herstellen können, die sich:

- Hinter persönlichen oder Netzwerk-Firewalls befinden
- In unterschiedlichen IP-Adressräumen befinden

ENC bietet eine virtuelle Netzwerkumgebung, in der Sie Verbindungen zwischen unterschiedlichen DSM-Komponenten herstellen können, die sich alle hinter verschiedenen Firewalls oder DMZs ("demilitarized zones") befinden. Dazu gehören Enterprise-Manager, Domänen-Manager, die Benutzeroberfläche, Scalability-Server und Agenten.

Wichtig! ENC kann nur von autorisierten und authentifizierten Anwendungen verwendet werden, um Verbindungen zu speziellen Endpunkten herzustellen, die bereits ENC-fähige Anwendungen für spezielle Zwecke installiert haben. ENC bietet keinen allgemeinen Durchgang durch die Firewall, der von anderen Anwendungen verwendet werden kann.

Wenn eine Verbindung zwischen zwei Computern hergestellt werden soll, dies jedoch normalerweise wegen einer Firewall nicht möglich ist, arrangiert ENC für beide Computer jeweils eine Verbindung zu einem dritten Computer (ENC-Router), der Daten zwischen den Computern weiterleitet.

Das ENC-Gateway bietet sichere Verbindungen über Firewalls hinweg. Folgende Bedingungen müssen dazu erfüllt sein:

- Alle Verbindungen über das virtuelle Netzwerk des ENC-Gateways müssen anhand von Zertifikaten ordnungsgemäß authentifiziert sein.
- Alle Verbindungen müssen ordnungsgemäß autorisiert sein. Die Autorisierungsregeln werden durch Richtlinien festgelegt, anhand derer konfiguriert wird, wer mit wem, wann und für welchen Vorgang eine Verbindung herstellen kann. Dies ist besonders wichtig bei Verbindungen über das öffentliche Netzwerk bzw. über das Internet.
- Alle Verbindungsversuche und sonstige Vorgänge können zum Zweck der Problembehebung und Sicherheit überwacht werden.

ENC-Komponenten

ENC verwendet CA IT Client Manager-spezifische Komponenten. Dazu gehören:

ENC-Client

Wird auf allen Computern mit ENC-Gateway ausgeführt und koordiniert alle Verbindungen, die Anwendungen über das ENC-Gateway-Netzwerk aufbauen. ENC-Clients halten eine Verbindung zum ENC-Gateway-Server aufrecht.

ENC-Gateway-Server

Dient als Scalability-Server für den ENC-Gateway, indem er Verbindungen und Registrierungen der ENC-Clients annimmt und sie an den ENC-Gateway-Manager weitergibt. In einem ENC-Netzwerk können mehrere Server verwendet werden.

ENC-Gateway-Manager

Richtet alle Verbindungen zwischen Endpunkten ein. Dem ENC-Gateway-Manager sind alle ENC-Gateway-Server, Clients und Router bekannt, da diese Komponenten sich beim Start registrieren. In einem ENC-Netzwerk darf nur ein ENC-Gateway-Manager vorhanden sein.

ENC-Gateway-Router

Leitet Daten zwischen Endpunkten weiter. In einem ENC-Netzwerk können mehrere Router verwendet werden.

Secure Socket Adapter

Stellt die Verbindung zwischen Anwendungen und dem ENC-Netzwerk dar. Er fängt Netzwerkaufrufe auf unterer Ebene ab und leitet sie, wenn möglich, an direkte Verbindungen um, anderenfalls an ENC-Verbindungen.

Hinweis: Der ENC-Gateway ist ein einziges Programm, das als Manager, Server, Router oder eine beliebige Kombination daraus fungieren kann. Der Manager besitzt immer auch einen Server. Die Rolle wird durch die folgenden Einstellungen im Konfigurationsspeicher (comstore) festgelegt: itrm/common/enc/server - MRS, SRS und Router. Wenn der Wert einer Einstellung 1 lautet, nimmt der Server die entsprechende Rolle an.

Unterstützte Plattformen

Die von ENC unterstützten Betriebssystemplattformen sind im Kapitel "Unterstützte Betriebssystemumgebungen" in den *Versionshinweisen zu CA IT Client Manager* aufgelistet, die in der Online-Dokumentation zu CA ITCM (Bookshelf) enthalten sind.

ENC-Gateway-Verbindungsprozess

Die ENC-Gateway-Funktionalität ermöglicht CA ITCM die Kommunikation mit Computern, die sich hinter einer Firewall befinden. Wenn eine Verbindung zwischen zwei Computern hergestellt werden soll, dies jedoch normalerweise wegen einer Firewall nicht möglich ist, sorgt der ENC-Gateway dafür, dass für beide Computer jeweils eine Verbindung zu einem dritten Computer hergestellt wird, der Daten zwischen den beiden Computern weiterleiten kann.

In einem ENC-Gateway-Netzwerk läuft der Verbindungsprozess zwischen zwei Endpunkten (Computern) wie folgt ab:

- Endpunkt 1 soll einen Port auf Verbindungen abhören. Es werden zwei Ports geöffnet, ein realer und ein virtueller. Der reale Port akzeptiert direkte Verbindungen. Der virtuelle Port wird vom ENC-Client unterhalten und hört ENC-Gateway-Verbindungen ab.
- Von Endpunkt 2 aus soll eine Verbindung hergestellt werden. Der Socket Adapter versucht, eine direkte Verbindung aufzubauen. Wenn dies erfolgreich ist (möglicherweise im selben Netzwerk), spielt der ENC-Gateway für den Prozess keine Rolle mehr.
- Schlägt der Verbindungsaufbau fehl, weist der Socket Adapter den ENC-Gateway-Manager an, eine Verbindung herzustellen.
- Der ENC-Gateway-Manager sendet eine Liste der bekannten ENC-Gateway-Router an beide Endpunkte. Die Endpunkte pingen die Router an und geben die Ergebnisse zurück. Der ENC-Gateway-Manager wählt einen Router aus, der für beide Endpunkte erreichbar ist, und weist die Endpunkte an, eine Verbindung zu ihm herzustellen.
- Die beiden Endpunkte stellen eine Verbindung zum ENC-Gateway-Router her, der anschließend Daten zwischen ihnen weiterleitet.

Dies setzt voraus, dass die Endpunkte eine nach außen gerichtete Verbindung von den Firewalls, hinter denen sich ihre Netzwerke befinden, zu ENC-Gateway-Servern und ENC-Gateway-Routern herstellen können. Nach innen gerichtete Verbindungen werden zu keinem Zeitpunkt hergestellt, daher müssen keine nach innen gerichteten Ports geöffnet werden.

ENC-Gateway-Sicherheit

Der ENC-Gateway ermöglicht eine sichere Kommunikation durch Firewalls hindurch, wobei die folgenden Sicherheitsmechanismen angewendet werden:

- Authentifizierung

  Alle ENC-Gateway-Knoten (Clients, Manager, Server und Router) müssen sich einander gegenseitig authentifizieren. Dazu wird TLS (Transport Layer Security) verwendet, eine aktualisierte Version von SSL. Diese Authentifizierungsmethode erfordert die Installation von Zertifikaten mit Hilfe der Microsoft PKI o. Ä.

- Autorisierung

  Alle ENC-Gateways werden mit einem Regelsatz konfiguriert, der die zulässigen Aktionen und die zeitlichen Abläufe bestimmt. Darin ist Folgendes enthalten:

  - Bereichszugehörigkeit von Knoten (analog zu NT-Gruppen, jedoch über verschiedene Netzwerke)
  - Weiße Liste der IP-Adressen. Dies ist eine Liste der IP-Adressen, für die das Herstellen von ENC-Gateway-Verbindungen zugelassen ist.
  - Regeln für das Zulassen oder das Verweigern der einzelnen ENC-Gateway-Vorgänge, wie z. B. das Verbinden und das Registrieren, basierend auf Bereichszugehörigkeit, Uhrzeit usw.
  - Zeitbereiche

Nach seiner Installation ist ein ENC-Gateway zunächst gesperrt. Er verfügt über keine Autorisierungsregeln und lehnt daher alle Verbindungen ab. Dies ist sinnvoll, da die Server in der Regel auf das Internet ausgerichtet sind. Dies kann zu Problemen führen, da CA ITCM zum Verwalten der Autorisierungsregeln verwendet wird und ein Domänen-Manager möglicherweise durch eine Firewall von dem Computer getrennt wird, auf dem der ENC-Gateway ausgeführt wird. Die Schritte zum Umgehen dieses Problems werden im Abschnitt "Bereitstellungsszenarios" beschrieben.

Authentifizierung

Beide Enden einer gesicherten Verbindung validieren (authentifizieren) das Zertifikat ihrer Peers (gegenseitige Authentifizierung) einschließlich der ausstellenden Zertifizierungsstelle.

Dazu ist es erforderlich, dass beide Parteien die Drittanbieter-Zertifizierungsstelle als vertrauenswürdig einstufen. ENC verwendet den Provider Microsoft SCHANNEL TLS und anschließend die WinTrust-Bibliothek, um zu erzwingen, dass das Zertifikat als vertrauenswürdig eingestuft wird. Die Vertrauenswürdigkeit der Root- und ggf. der Zwischenzertifikate wird durch das Betriebssystem mit Hilfe des Zertifikatspeichers und der APIs hergestellt.

ENC-Gateway-Autorisierungsregeln

Die virtuelle ENC-Infrastruktur wird durch Authentifizierung, Autorisierung und Auditing geschützt. Die Authentifizierung wird mit Hilfe des TLS-Protokolls ausgeführt, das dem Industriestandard entspricht. Sie wird in den Abschnitten Authentifizierung (siehe Seite 403) und ENC-Gateway-Authentifizierung (siehe Seite 469) beschrieben. Die Auditing-Komponente wird ebenfalls im Abschnitt Auditing von Ereignissen (siehe Seite 488) ausführlich dargestellt.

In diesem Abschnitt wird erläutert, wie und wo die Autorisierung verwendet wird. Der Abschnitt schließt mit einem Beispiel.

Allgemeine Begriffe

Nachfolgend sehen Sie eine Liste von Begriffen, die im Kontext der Autorisierungsregeln verwendet werden. Einige entsprechen dem Industriestandard, andere wurden für die Verwendung durch ENC angepasst.

Sicherheitsprinzipal

Ein Sicherheitsprinzipal ist ein authentifiziertes Objekt – in ENC immer ein Computer – das seine Identität den Gateway-Servern gegenüber nachgewiesen hat. Auf das Objekt wird immer mit dessen Uniform Resource Identifier (URI) verwiesen. Dieses Objekt ist die Entität, die eine Anfrage für den Zugriff auf ein gesichertes Objekt oder einen gesicherten Vorgang stellt. In ENC ist ein Sicherheitsprinzipal primär ein einzelner Computer, er kann jedoch auch durch einen Bereich (eine Gruppe) von Computern oder eine Untergruppe von Computern referenziert werden, der bzw. die durch eine Musterübereinstimmung mit der URI definiert wird.

Gesichertes Objekt

Das gesicherte Objekt ist das Ziel einer Zugriffsanforderung oder eines Vorgangs. Das gesicherte Objekt ist immer ein durch den URI benannter Computer. Die Zugriffsregeln können jedoch für einen einzelnen Computer, einen durch eine Musterübereinstimmung definierten Satz von Computern oder einen vollständigen Bereich gelten.

Bereich

Ein Bereich ist eine logische Gruppierung von Computern, die durch die Autorisierungskomponente auf einen Satz von Computern angewendet werden soll. In einem ausgegliederten Szenario repräsentiert ein Bereich in der Regel Computer auf Organisations- oder Organisationseinheitsebene. Sicherheitsprinzipale werden entweder durch eine genaue Übereinstimmung des URI oder durch Musterübereinstimmungen mit dem URI einem Bereich zugeordnet.

Musterübereinstimmung

ENC kann zum Festlegen der Bereichszugehörigkeit die Musterübereinstimmung verwenden. Die Musterübereinstimmung verwendet zum Ausführen des Übereinstimmungsalgorithmus reguläre Ausdrücke.

ENC verwendet PERL-kompatible reguläre Ausdrücke (PCRE, siehe http://www.pcre.org/) für die Musterübereinstimmung. Die vollständige PCRE-Syntax finden Sie unter http://perldoc.perl.org/perlre.html.

TACE – Zeitbasierter Zugriffssteuerungseintrag

Ein TACE ist eine Regel, die definiert, ob ein oder mehrere Vorgänge von einem Sicherheitsprinzipal zu einem bestimmten Zeitpunkt für ein gesichertes Objekt ausgeführt werden können. Einige Regeln verweigern den Zugriff, während andere den Zugriff gewähren. TACEs vom Typ "Verweigern" haben Vorrang vor TACEs vom Typ "Zulassen". Alle Vorgänge, die keine übereinstimmenden Regeln besitzen, werden implizit verweigert.

Wichtig! Die aktive Zeit eines Zugriffssteuerungseintrags ist immer die lokale Zeit des Ziels eines Vorgangs. Wenn eine Verbindung von einem Agenten zu einem anderen Agenten in einer anderen Zeitzone hergestellt werden soll, validiert der ENC-Gateway-Manager-Knoten den Zeitbereich im Kontext des Zielagenten.

TACL – Zeitbasierte Zugriffssteuerungsliste

Eine TACL ist eine Liste von TACE-Regeln.

Infrastrukturknoten

Dieser Begriff bezieht sich auf die ENC-Knoten, die die Infrastruktur des virtuellen ENC-Netzwerks bilden, einschließlich der Manager-, Server- und Router-Knoten, jedoch nicht auf die ENC-Agenten selbst.

URI – Uniform Resource Identifier

Ein URI ist eine Zeichenfolge, die zur Benennung oder Identifizierung einer Ressource verwendet wird. ENC verwendet einen URI zur Darstellung aller authentifizierter Objekte.

ENC und Uniform Resource Identifiers

Bei der ENC-Autorisierung werden Uniform Resource Identifiers (URIs) für die interne Datenbank verwendet. Ein ENC-URI hat das folgende Format:

```
x509cert://[TLS-SCHANNEL]/CN=forward,OU=computers,DC=forward,DC=com
```

x509cert

Gibt den Namespace an. "X509cert" bedeutet, dass der URI für ein x.509-Zertifikat steht.

[TLS-SCHANNEL]

Gibt die im URI eingebettete Autorität an. Dieser spezielle Name der Autorität zeigt, dass die Authentifizierung auf den Sicherheitsprovider TLS SCHANNEL und den WinTrust-Provider übergegangen ist. Diese Provider verwalten das Zertifikat für ENC.

CN=forward,OU=computers,DC=forward,DC=dom

Definiert den Namen des x.500-Subjekts als im Zertifikat eingebettet. Das tatsächliche Format und der Inhalt dieses Namens hängt vom Provider ab. Das oben stehende Beispiel stammt aus einem Zertifikat, das von den in Microsoft Active Directory integrierten Zertifizierungsdiensten erstellt wurde. Bei unterschiedlichen PKIs und der manuellen Zertifikaterstellung werden möglicherweise verschiedene Namenskonventionen verwendet.

Mit Hilfe des Hilfsprogramms "encUtilCmd" können Sie per Programmierung eine Computer-URI herausfinden. Wenn Sie "encUtilCmd certv" ausführen, werden die Zertifikatsidentitäten angezeigt, die der Computer für die ENC-Authentifizierung verwendet – ggf. sowohl für den Client als auch für den Server.

Beispiel: Befehl "encutilcmd certv"

```
C:\>encutilcmd certv
INFO: Aktueller Prozessbenutzer ist ein Mitglied der lokalen Administratorgruppe.
INFO: Clientseitiger TLS-Kontext  wurde erfolgreich erstellt und validiert.
URI: x509cert://[TLS-SCHANNEL]/CN=mach-02,CN=encserver,O=enc
INFO: Serverseitiger TLS-Kontext wurde erfolgreich erstellt und validiert.
URI: x509cert://[TLS-SCHANNEL]/CN=mach-02,CN=encserver,O=enc
```

Konfiguration von Autorisierungsregeln

Die Autorisierungsregeln für den ENC-Gateway-Dienst werden über den DSM-Konfigurationsrichtlinien-Editor konfiguriert. Anders als bei anderen Richtlinienabschnitten besteht kein direkter Zugriff auf die zugrunde liegenden Autorisierungstabellen, und die Konfiguration erfolgt über ein Dialogfeld. Das Dialogfeld verwaltet Abhängigkeiten zwischen Tabellen und führt eine Vorab-Evaluierung der angegebenen Regeln durch.

Die Konfigurationsansicht umfasst fünf Registerformate im Konfigurationsdialogfeld. Dies sind die Registerkarten und deren Inhalte:

Bereiche

Diese Ansicht bietet die Möglichkeit, einen ENC-Bereich anzuzeigen oder zu definieren und kurze Anmerkungen hinzuzufügen, die für den Bereich relevant sind.

Namenszuordnung

Diese Ansicht bietet die Möglichkeit, die Zuordnung zwischen authentifizierten Objekten und deren Bereichszugehörigkeit zu prüfen oder zu definieren. Das Schlüsselfeld enthält die authentifizierte Identität in Form eines URI. Die URI-Bereichszuordnung erfolgt über einen vollständig angegebenen URI, der genau übereinstimmen muss, oder einen als regulären Ausdruck angegebenen URI für eine Übereinstimmung mit mehreren URIs.

Zeitbereiche

Die gesamte Autorisierungszugriffssteuerung in ENC kann zeitlich beschränkt werden. Diese Registeransicht bietet die Möglichkeit, einen Zeitbereich zur Verwendung durch einzelne Zugriffssteuerungseinträge zu definieren. Einträge können entweder "normale Wochentage" sein, wobei der Zeitbereich für einen oder mehrere Tage zwischen Sonntag und Samstag gilt, oder "spezielle Daten", z. B. Neujahr usw.

Die Stunden, für die der Zeitbereich gültig ist, werden als Start- und Endzeit im 24-Stunden-Format angegeben, z. B. "00:00 - 00:00" für einen Zeitraum von vollen 24 Stunden. Der Zeitbereich kann in Schritten von 30 Minuten festgelegt werden, daher muss bei allen Einträgen der Minutenwert "00" oder "30" lauten.

Zugriffssteuerung

Diese Registerkarte bietet Zugriff auf die zeitbasierten Zugriffssteuerungseinträge. Jeder Eintrag ermöglicht Ihnen, benannte Regeln anzugeben, die Aktivitäten zulassen oder verweigern (Regeln, die den Zugriff verweigern, haben Vorrang vor Regeln, die den Zugriff zulassen). Der TACE-Name wird in Audit-Einträgen erfasst und auch durch den Hilfsprogramm-Befehl angezeigt, wenn Zugriffe auf Testregelsätze simuliert werden. Daher wird empfohlen, ggf. aussagefähige Namen für die einzelnen Regeln zu verwenden.

Der Zugriffssteuerungseintrag kann ein einzelnes Ereignis steuern oder aggregiert werden, um mehrere Ereignisse innerhalb einer einzigen Regel zu steuern. Für jede Regel gibt es eine geschützte Ressource, das gesicherte Objekt, und ein darauf zugreifendes Objekt, den Sicherheitsprinzipal.

IP-Adressen

Diese Registerkarte zeigt die Tabelle mit der weißen Liste der IP-Adressen an. Jeder Eintrag kann entweder eine einzelne IP-Adresse oder ein IP-Adressbereich sein, der durch einen Musterübereinstimmungs-Ausdruck angegeben wird. Die Infrastruktur-Computer akzeptieren nur Verbindungen von Computern mit den angegebenen Adressen.

Ereignisse

Die ENC-Infrastruktur definiert eine Reihe von Ereignissen, die Vorgängen entsprechen, die eine Autorisierungsprüfung erfordern. Die meisten dieser Ereignisse können in einem TACE festgelegt werden, um zu steuern, welche Aktionen von Sicherheitsprinzipalen zu welchem Zeitpunkt zugelassen werden. In den meisten Fällen wird die physische Verbindung beendet, wenn die Autorisierungskomponente die Zugriffsanforderung ablehnt. Die Ereignisse "Namensabfrage" und "Agentenverbindung" stellen eine Ausnahme dar.

Nachfolgend werden die einzelnen Ereignisse der Reihe nach kurz beschrieben. Für jedes Ereignis definiert der Eintrag "Gesichertes Objekt" die geschützte Ressource und der Eintrag "Sicherheitsprinzipal" die anfordernde Ressource.

Netzwerkverbindung

Gesichertes Objekt: Der ENC-Knoten, der die Verbindung empfängt.

Dies ist das einzige Ereignis, das nicht innerhalb einer TACE-Regel gesteuert wird. Daher ist das Ziel des Vorgangs implizit. Jeder Zugriff auf die Infrastruktur wird durch die weiße Liste der IP-Adressen gesteuert. Das Herstellen einer Verbindung zu den ENC-Infrastrukturknoten wird nur Knoten oder IP-Bereichen erlaubt, die in der weißen Liste der IP-Adressen aufgelistet sind. Das gesicherte Objekt in dieser Instanz ist immer der Ziel-ENC-Knoten. Die weiße Liste gilt derzeit für alle ENC-Infrastrukturknoten.

Authentifizierte Verbindung

Gesichertes Objekt: Der ENC-Knoten, der die Verbindung akzeptiert.

Sicherheitsprinzipal: Die authentifizierte Identität des verbundenen ENC-Knotens.

Alle Knoten müssen sich authentifizieren, sobald sie eine Netzwerkverbindung zu einem Partner-ENC-Knoten hergestellt haben. Dieses Ereignis wird generiert, sobald eine erfolgreiche Authentifizierungssequenz abgeschlossen wurde. Der akzeptierende ENC-Knoten ruft die Autorisierungs-API mit dem authentifizierten URI des verbindenden Knotens auf, um festzustellen, ob der Vorgang zugelassen wird.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder als Bereichsnamen angeben.

Serverregistrierung

Gesichertes Objekt: Der ENC-Gateway-Manager-Knoten.

Sicherheitsprinzipal: Die authentifizierte Identität des ENC-Gateway-Server-Knotens.

Wenn ein ENC-Gateway-Server erfolgreich eine authentifizierte Verbindung zu seinem Manager herstellt, sendet er eine Registrierungsmeldung mit einer Anfrage für die Registrierung als Server. Der ENC-Gateway-Manager ruft anschließend die Autorisierungskomponente auf, um festzustellen, ob die Registrierung des Servers bei diesem Manager zugelassen wird. Dadurch wird verhindert, dass nicht autorisierte ENC-Gateway-Server in das virtuelle ENC-Netzwerk aufgenommen werden.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder als Bereichsnamen angeben.

Router-Registrierung

Gesichertes Objekt: Der ENC-Gateway-Server, der die Anfrage verarbeitet.

Sicherheitsprinzipal: Die authentifizierte Identität des ENC-Gateway-Router-Knotens.

Wenn ein Router erfolgreich eine authentifizierte Verbindung zu seinem Server herstellt, sendet er ebenfalls eine Registrierungsmeldung mit einer Anfrage für die Registrierung als Router. Der ENC-Gateway-Server führt eine lokale Autorisierungsprüfung durch, um festzustellen, ob dieser Vorgang zugelassen wird, und leitet die Anfrage anschließend zur weiteren Autorisierung an den ENC-Gateway-Manager weiter.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder als Bereichsnamen angeben.

Manager-Router-Registrierung

Gesichertes Objekt: Der ENC-Gateway-Manager-Knoten.

Sicherheitsprinzipal: Die authentifizierte Identität des ENC-Gateway-Router-Knotens.

Dieses Ereignis wird generiert, wenn ein Server eine Router-Registrierungsmeldung weiterleitet. Der ENC-Gateway-Manager ruft die Autorisierungskomponente auf, um festzustellen, ob die Aufnahme des Routers in das virtuelle ENC-Netzwerk zugelassen wird.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder als Bereichsnamen angeben.

Server-Client-Registrierung

Gesichertes Objekt: Der ENC-Gateway-Server, der die Anfrage verarbeitet.

Sicherheitsprinzipal: Die authentifizierte Identität des ENC-Client-Knotens.

Dieses Ereignis wird generiert, wenn sich ein ENC-Client-Knoten auf einem ENC-Gateway-Server-Knoten registriert. Der Server führt eine lokale Autorisierungsprüfung durch und leitet die Registrierungsanfrage anschließend für eine Autorisierungsantwort an den ENC-Gateway-Manager weiter.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder als Bereichsnamen angeben.

Manager-Client-Registrierung

Gesichertes Objekt: Der ENC-Gateway-Manager-Knoten.

Sicherheitsprinzipal: Die authentifizierte Identität des ENC-Client-Knotens.

Dieses Ereignis wird generiert, wenn ein ENC-Gateway-Server-Knoten eine ENC-Client-Registrierungsmeldung an den ENC-Gateway-Manager weiterleitet.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder als Bereichsnamen angeben.

Überwachung durch Host

Dieses Ereignis ist derzeit nicht implementiert. Das Ereignis ist eine lokale Agenten-Autorisierungsprüfung, um festzustellen, ob das Herstellen einer Überwachungsverbindung durch den ENC-Agenten zugelassen wird.

Hostverbindung

Dieses Ereignis ist derzeit nicht implementiert. Das Ereignis ist eine lokale Agenten-Autorisierungsprüfung, um festzustellen, ob das Herstellen einer ausgehenden Verbindung durch den ENC-Agenten zugelassen wird.

Agentenverbindung

Gesichertes Objekt: Die Sicherheitsidentität des Ziel-ENC-Knotens.

Sicherheitsprinzipal: Die authentifizierte Identität des anfordernden ENC-Client-Knotens.

Dieses Ereignis wird auf dem ENC-Gateway-Manager-Knoten generiert, wenn eine Verbindung von einem ENC-Agenten zu einem anderen ENC-Agentenknoten hergestellt werden soll.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder als Bereichsnamen angeben.

Agentenverbindung zum Router

Gesichertes Objekt: Die Sicherheitsidentität des ENC-Gateway-Router-Knotens.

Sicherheitsprinzipal: Die authentifizierte Identität des anfordernden ENC-Client-Knotens.

Dieses Ereignis wird auf dem ENC-Gateway-Router-Knoten generiert, wenn ein ENC-Agent eine Verbindung zu dem Router herstellt, um eine virtuelle Verbindung zu einem anderen ENC-Agentenknoten zu schaffen.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder als Bereichsnamen angeben.

Namensabfrage

Gesichertes Objekt: Die Sicherheitsidentität des Ziel-ENC-Knotens.

Sicherheitsprinzipal: Die authentifizierte Identität des anfordernden ENC-Client-Knotens.

Dieses Ereignis wird auf dem ENC-Gateway-Manager-Knoten generiert, wenn von einem ENC-Knoten ein Namensabfragevorgang ausgeführt werden soll, um einen symbolischen Hostnamen in eine private ENC-Adresse zu konvertieren.

Der ENC-Gateway-Manager extrahiert zunächst den Ziel-DNS-Namen aus der Anforderung für die Namensabfrage und konvertiert diesen in einen oder mehrere Client-Datensätze (wodurch doppelte Hostnamen in verschiedenen Bereichen, jedoch nicht innerhalb eines Bereichs zugelassen werden). Diese Client-Datensätze werden an die Autorisierungskomponente weitergeleitet, die entscheidet, ob die Anforderung für die Namensabfrage zugelassen werden soll. Ein Client-Datensatz besteht aus dem bekannten DNS-Namen und der authentifizierten Identität des Objekts.

Der Zugriffssteuerungseintrag für dieses Ereignis kann das Ziel als literale Computer-Identität (von der Authentifizierung), als Bereichsnamen oder als Musterübereinstimmungsausdruck zum Ansprechen einer Untergruppe von Computern oder sogar mehrerer Bereiche angeben.

Verwaltungszugriff

Gesichertes Objekt: Die Sicherheitsidentität des Ziel-ENC-Knotens.

Sicherheitsprinzipal: Die authentifizierte Identität des anfordernden ENC-Client-Knotens.

Dieses Ereignis wird generiert, wenn eine ENC-Client-Verbindung Management-Informationen vom Ziel-ENC-Gateway anfordert.

Die Management-Informationen können Daten zu allen virtuellen ENC-Verbindungen umfassen, die von einem ENC-Server beherbergt werden, daher darf nur bestätigten Knoten Zugriff erteilt werden.

Verbindungssequenz

In diesem Abschnitt wird die allgemeine Funktionalität beschrieben, die alle ENC-Knoten ausführen müssen, um in die virtuelle ENC-Infrastruktur aufgenommen zu werden. Die allgemeine Funktionalität wird in drei verschiedene Phasen unterteilt: die physische Verbindung, die Authentifizierung und schließlich die Autorisierung.

Physische Verbindung

Alle Knoten müssen in der Tabelle mit der weißen Liste der IP-Adressen aufgelistet sein, damit in der ersten Instanz zugelassen wird, dass sie eine Verbindung zum Ziel-ENC-Knoten herstellen. Für jede zu einem ENC-Knoten hergestellte Verbindung wird die Autorisierungskomponente aufgerufen, um zu prüfen, ob der Zugriff erlaubt oder verweigert werden soll. Wenn der Zugriff verweigert wird, wird die Verbindung sofort beendet.

Authentifizierung

Sobald eine Netzwerkübertragungsverbindung hergestellt wurde, verwenden beide an der Kommunikation beteiligten Peers das TLS-Protokoll, um sich gegenseitig zu authentifizieren und über eine vertrauenswürdige Drittanbieter-Zertifizierungsstelle zu validieren, ob die authentifizierte Identität vertrauenswürdig und derzeit gültig ist.

Autorisierung

Im Anschluss an die Authentifizierungphase wird die authentifizierte Identität zur Ereignisprüfung 'Authentifizierte Verbindung' an die Autorisierungskomponente weitergeleitet. Das gesicherte Objekt für dieses Ereignis ist der Ziel-ENC-Knoten. Es kann eine Zugriffsregel zum Zulassen (oder Verweigern) dieses Vorgangs mit dem einzelnen Computer als gesichertes Objekt, mit einer Gruppe von Computernamen, die über einen Musterübereinstimmungsausdruck angegeben wurde, oder über die Bereichszugehörigkeit angegeben werden.

Fehler in der oben angegebenen Sequenz werden durch das Sicherheitsüberwachungs-Subsystem aufgezeichnet, wenn die entsprechende Kategorie oder Meldungen aktiviert sind. Die Überwachungskomponente kann auch so konfiguriert werden, dass sie ebenfalls alle erfolgreichen Vorgänge aufzeichnet.

Alle ENC-Knoten, egal, ob Server, Router oder Client-Agent, führen eine Registrierung auf den Knoten durch, zu denen sie eine Verbindung herstellen. Für jeden Registrierungstyp wird ein separates Ereignis definiert, da es nur ENC-Gateway-Server-Knoten erlaubt werden soll, einen Serverregistrierungsvorgang durchzuführen, nur ENC-Gateway-Router eine Router-Registrierung durchführen dürfen usw.

Abhängig von Ihrer Infrastruktur können Sie einzelne Zugriffssteuerungseinträge für jedes Ereignis und/oder jedes gesicherte Objekt erstellen oder Ereignisse und Computer innerhalb eines Bereichs in Gruppen zusammenfassen, um eine gröber strukturierte Zugriffssteuerung zu erhalten.

Virtuelle ENC-Verbindungen

Nachdem nun alle physischen ENC-Infrastrukturknoten normal arbeiten, betrachten wir das Betriebsverhalten des virtuellen ENC-Netzwerks. Im Standardzustand werden keine Verbindungen oder Namensabfragen über das Netzwerk zugelassen, es sei denn, es sind explizite Zugriffssteuerungseinträge vorhanden, die dies zulassen. Auch bei Computern, die innerhalb einer Bereichszuordnung zusammengefasst wurden, wird nicht automatisch zugelassen, dass sie sich gegenseitig sehen oder eine Verbindung miteinander herstellen können.

Wenn die Kommunikation von einem ENC-Agentenknoten mit einem anderen ENC-Agentenknoten ermöglicht werden soll, findet als erster Vorgang in der Regel ein Namensabfrage-Ereignis statt. In den meisten Fällen ist nur ein registrierter Computer mit dem entsprechenden Namen vorhanden, und dieser befindet sich in der Regel im selben Bereich wie der anfordernde Computer, so dass für ihn eine umfassende Zugriffssteuerungsregel gilt, die allen ENC-Knoten innerhalb eines bestimmten Bereichs ermöglicht, mit anderen Mitgliedern seines Bereichs in Kontakt zu treten und Abfragen für sie durchzuführen. In seltenen Fällen können zwei oder mehr Computer mit demselben vollständig qualifizierten Namen vorhanden sein. In diesem Fall muss die Namensabfrage eindeutig gemacht werden, indem sichergestellt wird, dass nur Verweise auf Computer entfernt werden können, die sich innerhalb desselben Bereichs (bzw. Bereiche) befinden wie das anfordernde Objekt. Dies soll sicherstellen, dass kein unbeabsichtigter Datenaustausch zwischen Bereichen auftreten kann, sofern dies nicht explizit durch eine Zugriffsregel zugelassen wird.

Wenn die Autorisierungskomponente die Anforderung für die Namensabfrage zulässt, wird die IP-Adresse des virtuellen ENC-Hosts an den ENC-Client-Agenten zurückgegeben. Der ENC-Client gibt anschließend eine Agentenverbindungsanforderung an den ENC-Gateway-Server/-Manager aus. Der ENC-Gateway-Manager fragt wieder die gesicherte Identität ab, die der Adresse dieser Anforderung zugeordnet ist, und ruft das Autorisierungssystem auf, damit dieses den auszuführenden Vorgang genehmigt.

Wenn die Genehmigung für die Verbindung erteilt wird, stellen beide Agenten – die Peers der virtuellen Kommunikationsverbindungen – eine Verbindung zu ENC-Gateway-Routern her, um die Verbindung fertig zu stellen. Diese Verbindung wird wieder authentifiziert, und die Autorisierung zum Zugriff auf den Router wird angefordert.

Beispiel für das Festlegen von Regeln

In diesem Beispiel wird für die Beschreibung der Autorisierungsregeln die Dateidefinition aus dem Befehlszeilen-Hilfsprogramm "encUtilCmd" verwendet. Für den DSM-Explorer gilt jedoch Entsprechendes, da die Regelsätze einander sehr ähnlich sind.

Mit dem Hilfsprogramm "encUtilCmd" und dem Befehl 'create' ist es möglich, einen einfachen Satz von Regeln zu generieren, die den unten beschriebenen ähneln. Dies bietet ebenfalls die Möglichkeit, gleichzeitig ein Testskript zum Ausprobieren der Regeln zu generieren.

In diesem Beispiel werden die folgenden Bereiche verwendet:

[Infrastruktur]

Dieser Bereich wird zum Aufbewahren aller Infrastrukturknoten (Manager, Server, Router usw.) verwendet. Die ENC-Infrastruktur wird durch Forward, Inc. verwaltet. In diesem Beispiel wird der Bereichsname zu seiner Hervorhebung in Klammern gesetzt, dies ist jedoch nicht erforderlich. Alle Bereichsnamen sind gleichwertig. Alle Infrastrukturcomputer besitzen Zertifikatsnamen mit dem gemeinsamen RDN (Relative Distinguished Name) "DC=forwardinc,DC=com".

[dsm]

Dies ist ein Beispielbereich, der alle Computer enthält, die zusammen die DSM-Infrastruktur bilden. Wir unterscheiden im Kontext zwischen der ENC-Infrastruktur und der DSM-Infrastruktur, um die Abgrenzung zwischen den Bereichen deutlicher zu machen. Alle DSM-Computer besitzen Zertifikatsnamen mit dem RDN "DC=forward-dsm,DC=com".

east

Dies ist ein Beispielbereich, der alle Computer des Unternehmens 'east' enthält. Alle 'east'-Computer besitzen Zertifikatsnamen mit dem RDN "DC=east,DC=com".

west

Dies ist ein weiterer Beispielbereich, der alle Computer des Unternehmens 'west' enthält. Alle 'west'-Computer besitzen Zertifikatsnamen mit dem RDN "DC=west,DC=com".

In diesem Beispiel werden die ENC-Knoten, da sie ebenfalls mindestens DSM-Agentenknoten sind, als eigenständige Geräte behandelt, die von den DSM-Knoten getrennt sind. In der DSM-ENC-Umgebung besteht in der Regel die Anforderung, dass DSM-Bereichsknoten alle Knoten innerhalb einzelner Bereiche sehen und eine Verbindung zu ihnen herstellen können und dass Bereichsagenten Verbindungen zu Knoten im DSM-Bereich herstellen können, dass jedoch Mitglieder eines verwalteten Bereichs Mitglieder eines anderen verwalteten Bereichs nicht sehen oder eine Verbindung zu ihnen herstellen können.

Sie müssen nun damit beginnen, Autorisierungsregeln zu definieren, damit die Infrastruktur kommunizieren kann und die Bereichscomputer Verbindungen herstellen und das virtuelle Netzwerk verwenden können. In der ersten Instanz müssen Sie die Bereiche deklarieren, damit diese verwendet und mit Querverweisen versehen werden können.

Nachfolgend sehen Sie einen Auszug für die Autorisierungsregeldatei: den Abschnitt "realm". Er definiert die vier oben genannten Bereiche.

```
realm
{Name "[Infrastruktur]" Hinweise "ENC-Infrastrukturbereich"}
{Name "[dsm]" Hinweise "Der DSM-Infrastrukturbereich"}
{Name "east" Hinweise "Kontakt von East Inc. ist admin@east.com"}
{Name "west" Hinweise "Kontakt von West Inc. ist admin@west.com"}
end
```

Der nächste Schritt besteht darin, die Zuordnung zwischen Zertifikats-URIs und den Bereichen selbst zu definieren. In diesem Beispiel wird für alle Einträge die Musterübereinstimmung verwendet.

```
URIMapping
{URI ".*,DC=forwardinc,DC=com" Enabled "1" Type "Pattern" Realm
"[Infrastruktur]"}
{URI ".*,DC=forward-dsm,DC=com" Enabled "1" Type "Pattern" Realm "[dsm]"}
{URI ".*,DC=east,DC=com" Enabled "1" Type "Pattern" Realm "east"}
{URI ".*,DC=west,DC=com" Enabled "1" Type "Pattern" Realm "west"}
end
```

Als Nächstes beschäftigen Sie sich mit der weißen Liste der IP-Adressen. In diesem Beispiel lassen Sie für zwei öffentliche IPv4-Subnetze den Zugriff auf die ENC-Infrastruktur zu.

```
IPAddWhiteList
{IPAddress "130\.119\..+" enabled "1" Type "Pattern"}
{IPAddress "141\.202\..+" enabled "1" Type "Pattern"}
{IPAddress "131\.119\..+" enabled "1" Type "Pattern"}
end
```

Das letzte Element, das erstellt werden muss, bevor Sie mit den einzelnen Zugriffssteuerungseinträgen fortfahren, ist ein aktiver Zeitbereich. Für die Zwecke dieses Beispiels ist der Zeitbereich für alle Wochentage aktiv und umfasst alle 24 Stunden eines Tages.

```
TimeRange
{Name "Alle Tage" enabled "1" Hours "00:00 - 00:00" Type "normal" Weekdays
"sunday - saturday"}
end
```

Jetzt sind alle grundlegenden Elemente vorhanden, die Sie benötigen, um mit den Zugriffsregeln fortzufahren. Sie können sich nun auf die Zugriffssteuerungseinträge selbst konzentrieren. In diesem Beispiel verwenden Sie für mehr Klarheit hauptsächlich einzelne Zugriffssteuerungseinträge. Unter realen Bedingungen kann es einfacher und effizienter sein, mehrere Regeln zu einer einzigen Regel zusammenzufassen.

Nachfolgend sehen Sie nur zu Beispielzwecken einen einzelnen Zugriffssteuerungseintrag. Alle hier beschriebenen Regeln müssen wie nachfolgend dargestellt zwischen den Tags "TimeACL" und "end" definiert oder in der Konfigurations-UI erstellt werden.

Diese Regel mit dem Namen "AC-[Infrastruktur]-[Infrastruktur]" definiert einen Eintrag, der allen Mitgliedern des Infrastrukturbereichs erlaubt, auf andere Mitglieder des Infrastrukturbereichs zuzugreifen und sich bei ihnen zu authentifizieren. Sie referenziert den Zeitbereich 'Alle Tage', den Sie zuvor definiert haben, und ist daher jeden Tag den ganzen Tag lang aktiv.

```
TimeACL
{Name "AC-[Infrastruktur]-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange
"Alle Tage" SecPrincType "realm" SecPrinc "[Infrastruktur]" SecObjType "realm"
SecObj "[Infrastruktur]" Events "AuthenticatedConnection"}
...
end
```

Sie müssen ähnliche Regeln für die anderen Bereiche hinzufügen, in diesem Fall für '[dsm]', 'east' und 'west'. Die Regeln sind mit den oben angegebenen Regeln identisch, abgesehen davon, dass der Sicherheitsprinzipal in den dieser anderen Bereiche geändert wird, wie nachfolgend dargestellt.

```
{Name "AC-[dsm]-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj
"[Infrastruktur]" Events "AuthenticatedConnection"}
{Name "AC-east-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj
"[Infrastruktur]" Events "AuthenticatedConnection"}
{Name "AC-west-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj
"[Infrastruktur]" Events "AuthenticatedConnection"}
```

Jetzt definieren Sie weitere Infrastruktureinträge. Zu den Einträgen gehören Kommentare, die ihren Zweck angeben. Wie zuvor erwähnt, wäre es möglich, diese zu einem einzigen Eintrag zu rationalisieren, bei dem das Feld "Events" auf "ManagerRegisterServer ServerRegisterRouter ManagerRegisterRouter ManagerRegisterAgent" gesetzt wird. Das Trennen der Regeln besitzt den Vorteil, dass die Verifizierungstools und die Auditing-Protokollierung innerhalb der ENC-Subsysteme den eindeutigen Regelnamen verwenden, wenn sie aufzeichnen, warum ein Vorgang zugelassen oder nicht zugelassen wurde.

```
; Dieser Eintrag ermöglicht, dass alle Infrastrukturknoten einen Server beim
Manager registrieren können.
{Name "MRS-[Infrastruktur]-[Infrastruktur]" enabled "1" RuleType "allow"
TimeRange "Alle Tage" SecPrincType "realm" SecPrinc "[Infrastruktur]" SecObjType
"realm" SecObj "[Infrastruktur]" Events "ManagerRegisterServer"}
;
; Dieser Eintrag ermöglicht, dass alle Infrastrukturknoten einen Router bei einem
Server registrieren können.
{Name "SRR-[Infrastruktur]-[Infrastruktur]" enabled "1" RuleType "allow"
TimeRange "Alle Tage" SecPrincType "realm" SecPrinc "[Infrastruktur]" SecObjType
"realm" SecObj "[Infrastruktur]" Events "ServerRegisterRouter"}
;
; Dieser Eintrag ermöglicht, dass alle Infrastrukturknoten einen Router beim
Manager registrieren können.
{Name "MRR-[Infrastruktur]-[Infrastruktur]" enabled "1" RuleType "allow"
TimeRange "Alle Tage" SecPrincType "realm" SecPrinc "[Infrastruktur]" SecObjType
"realm" SecObj "[Infrastruktur]" Events "ManagerRegisterRouter"}
;
; Dieser Eintrag ermöglicht, dass alle Infrastrukturknoten einen Client beim
Manager registrieren können.
{Name "MRA-[Infrastruktur]-[Infrastruktur]" enabled "1" RuleType "allow"
TimeRange "Alle Tage" SecPrincType "realm" SecPrinc "[Infrastruktur]" SecObjType
"realm" SecObj "[Infrastruktur]" Events "ManagerRegisterAgent"}
```

Jetzt müssen Sie die Möglichkeit zur Registrierung auf den Infrastrukturknoten für die DSM und die verwalteten Bereiche deklarieren. Die folgenden Einträge liefern diese Konfiguration.

```
{Name "SRA-[dsm]-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj
"[Infrastruktur]" Events "ServerRegisterAgent"}

{Name "SRA-east-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj
"[Infrastruktur]" Events "ServerRegisterAgent"}

{Name "SRA-west-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj
"[Infrastruktur]" Events "ServerRegisterAgent"}
```

Die ENC-Gateway-Router erfordern außerdem eine Autorisierungskonfiguration für alle Knoten, die mit ihnen verbunden und durch sie geroutet werden. Die folgenden Einträge definieren dies.

```
; Diese Einträge ermöglichen, dass alle DSM-Knoten eine Verbindung zu Routern im
Infrastrukturbereich herstellen können.
{Name "RAC-[dsm]-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj
"[Infrastruktur]" Events "RouterAgentConnect"}

; Diese Einträge ermöglichen, dass alle Agentenknoten der genannten Bereiche eine
Verbindung zu Routern im Infrastrukturbereich herstellen können.
{Name "RAC-east-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj
"[Infrastruktur]" Events "RouterAgentConnect"}
{Name "RAC-west-[Infrastruktur]" enabled "1" RuleType "allow" TimeRange "Alle
Tage" SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj
"[Infrastruktur]" Events "RouterAgentConnect"}
```

Sie verfügen nun über eine ausreichende Menge an Konfigurationsdaten, um allen ENC-Knoten aus der DSM und den verwalteten Bereichen zu ermöglichen, Verbindungen zu allen Knoten in der ENC-Infrastruktur herzustellen, sich bei ihnen zu authentifizieren und sich auf ihnen zu registrieren. Der nächste Schritt besteht darin, die Namensabfrage- und die Agentenverbindungs-Funktionalität zuzulassen. Die folgenden Einträge definieren dies.

Es gibt für die Regeln für alle Knoten Entsprechungen: Die verwalteten Bereiche dürfen die Namen aller mit DSM ENC verbundenen Computer abfragen. Die mit DSM ENC verbundenen Computer wiederum dürfen die Namen aller Mitglieder der verwalteten Bereiche abfragen. Die Regeln und ihre Entsprechungen müssen explizit wie unten dargestellt angegeben werden.

Beachten Sie, dass es keine Regeln gibt, mit denen es 'east' ermöglicht wird, 'west' zu sehen, und umgekehrt auch keine Regeln, mit denen es 'west' ermöglicht wird, 'east' zu sehen. Deshalb sind keine Abfragen von einem Bereich zum anderen möglich. Diese Namespace-Trennung ist für den sicheren Betrieb des virtuellen Netzwerks ausschlaggebend.

```
; Diese Einträge ermöglichen, dass alle Agentenknoten der genannten Bereiche
Abfragen nach ENC-Mitgliedern im DSM-Bereich durchführen können.
{Name "NL-east-[dsm]" enabled "1" RuleType "allow" TimeRange "Alle Tage"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events
"ManagerNameLookup"}
{Name "NL-west-[dsm]" enabled "1" RuleType "allow" TimeRange "Alle Tage"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events
"ManagerNameLookup"}

; Diese Einträge ermöglichen, dass alle DSM-Knoten Abfragen nach ENC-Mitgliedern
in den genannten Bereichen durchführen können.
{Name "NL-[dsm]-east" enabled "1" RuleType "allow" TimeRange "Alle Tage"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events
"ManagerNameLookup"}
{Name "NL-[dsm]-west" enabled "1" RuleType "allow" TimeRange "Alle Tage"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events
"ManagerNameLookup"}
```

Die folgenden Einträge ermöglichen den Agenten, Verbindungen zu und von der DSM und den verwalteten Bereichen herzustellen. Es wäre wiederum möglich gewesen, diese Einträge mit dem vorherigen Regelsatz zu kombinieren, die Trennung ermöglicht jedoch eine detailliertere Protokollierung und Problembehebung für die Regeln.

```
; Diese Einträge ermöglichen, dass alle Agentenknoten der genannten Bereiche eine
Verbindung zu ENC-Mitgliedern im DSM-Bereich herstellen können.
{Name "ACN-east-[dsm]" enabled "1" RuleType "allow" TimeRange "Alle Tage"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events
"AgentConnect"}
{Name "ACN-west-[dsm]" enabled "1" RuleType "allow" TimeRange "Alle Tage"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events
"AgentConnect"}

; Diese Einträge ermöglichen allen DSM-Knoten, eine Verbindung zu ENC-Mitgliedern
in den benannten Bereichen herzustellen.
{Name "ACN-[dsm]-east" enabled "1" RuleType "allow" TimeRange "Alle Tage"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events
"AgentConnect"}
{Name "ACN-[dsm]-west" enabled "1" RuleType "allow" TimeRange "Alle Tage"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events
"AgentConnect"}
```

Damit ist der Beispiel-Regelsatz abgeschlossen.

Fragen zur Vorgehensweise

In diesem Abschnitt soll versucht werden, mögliche Fragen vorwegzunehmen und kurz und bündig zu beantworten.

Ich verwende die spezielle Mitgliedschaft für alle Bereiche (*), die Zeitbereiche werden jedoch nicht berücksichtigt. Woran liegt das?

Die Übereinstimmung mit "*" markiert das Computerobjekt als Mitglied aller Bereiche und impliziert außerdem, dass es sich um einen "super-user" handelt. Ein Objekt mit Superuser-Zugriff kann alle Vorgänge ausführen. Daher lässt das Autorisierungs-Subsystem den angegebenen Vorgang immer zu, unabhängig von Zeit- oder Zugriffsbeschränkungen. Ein Superuser-Bereich unterliegt hinsichtlich der von ihm ausgeführten Vorgänge keinen Einschränkungen, er kann z. B. beliebig Verbindungen herstellen und Abfragen durchführen. Beachten Sie, dass die Verwendung des Superuser-Typs mit einer Warnung im Systemanwendungsprotokoll überwacht wird.

Gibt es eine Möglichkeit, Regeln vor ihrer Anwendung zu prüfen?

Ja. Verwenden Sie hierzu den ENC-Hilfsprogramm-Befehl "encUtilCmd" und den Befehl 'verify'. Hiermit können Sie alle vorausgehend aufgelisteten Ereignisse simulieren. Genaue Anweisungen zur Verwendung der Anwendung finden Sie im Referenzhandbuch zu "encUtilCmd".

Ich muss eine große Anzahl von Regeln erstellen. Gibt es dazu eine einfachere Möglichkeit?

Ja. Verwenden Sie auch hierzu den ENC-Hilfsprogramm-Befehl "encUtilCmd". Mit dem Befehl 'create' können Sie einen Regelsatz für mehrere Bereiche erstellen, und er definiert einen grundlegenden Satz von Regeln, der den Ansatz in diesem Dokumentabschnitt widerspiegelt. Sie können gleichzeitig auch ein Testskript erstellen, das alle erstellten Regeln mit Hilfe von simulierten Identitäten verifiziert. Sie können anschließend die generierten Regeln dahingehend ändern, dass sie die echten Sicherheitsidentitäten verwenden, und andere Bereiche auf Ihre speziellen Anforderungen abstimmen.

Auditing von Ereignissen

Der ENC-Gateway überwacht intern Ereignisse auf den Verbindungen zwischen Knoten und generiert im Ereignisprotokoll des Betriebssystems Audit-Informationen. Diese können optional auch an das Event Management-System oder eine Textdatei gesendet werden. Audit-Ereignisse werden in Kategorien unterteilt, die sich auf Fehler, Verbindungen, Sicherheit usw. beziehen. Ereignisse können einzeln oder nach Kategorien aktiviert oder deaktiviert werden.

Standardmäßig sind alle Audit-Kategorien außer der Fehlerkategorie deaktiviert, obwohl alle Meldungen innerhalb ihrer Kategorien aktiviert sind. Dies verhindert, dass das Ereignisprotokoll mit ENC-Ereignissen überflutet wird. Der Administrator sollte Ereignisse bei der Problembehebung oder der Überwachung des Systembetriebs bei Bedarf aktivieren.

Audit-Ereignisse können aktiviert werden, indem die entsprechende Kategorie aktiviert wird, oder es können alle Audit-Ereignisse durch das Festlegen eines einzigen Parameters aktiviert werden.

Beachten Sie ebenfalls, dass standardmäßig alle Audit-Konfigurationsdaten lokal verwaltet werden, jedoch mit Hilfe des Richtlinien-Editors im DSM-Explorer leicht auf die zentrale Verwaltung umgestellt werden können.

Eine vollständige Liste der Ereigniskategorien finden Sie unter dem Thema "Richtliniengruppe 'ENC-Gateway-Server- und -Client-Auditing'" im Abschnitt "Konfigurationsrichtlinie" der *DSM-Explorer-Hilfe*.

Installation und Konfiguration von ENC-Gateway-Komponenten

Die Installation der ENC-Gateway-Funktionalität wird durch den Installer von CA IT Client Manager unterstützt. Dies gilt derzeit nur für Windows-Betriebsumgebungen.

Die Konfiguration der ENC-Gateway-Komponenten erfolgt über Parameter im Konfigurationsspeicher (comstore) und wird als verwaltete Konfigurationsrichtlinie gepusht.

Die ENC-Gateway-Funktionalität ist standardmäßig deaktiviert, da angenommen wird, dass sich die Mehrheit der CA IT Client Manager-Installationen innerhalb von Unternehmensnetzwerken befinden und das Internet oder interne Firewalls nicht durchlaufen werden müssen.

Hinweis: Wenn Sie einen Webserver wie IIS oder Apache auf demselben Computer ausführen möchten wie einen ENC-Gateway-Server, müssen diese so konfiguriert sein, dass sie nicht versuchen, dieselben Ports zu öffnen. Standardmäßig hört ENC Port 80 und 443 ab. IIS und Apache hören ebenfalls Port 80 ab. IISadmin hört Port 443 ab. Wenn ein Port-Konflikt auftritt und ENC die Ports nicht abhören kann, veranlasst es im Systemereignisprotokoll ein entsprechendes Ereignis.

ENC- und SSA-Konfiguration

Die Konfiguration von ENC-Komponenten erfolgt über allgemeine Konfigurationsparameter und wird durch eine verwaltete Konfigurationsrichtlinie gepusht. Wenn die Konfigurationsrichtlinie für ENC oder SSA geändert wird, kann dies einen Neustart von SSA PMUX und CAM verursachen. Weitere Informationen zu den ENC-Konfigurationsrichtlinien finden Sie unter "Richtliniengruppe 'ENC-Gateway'" im Abschnitt "Konfigurationsrichtlinie" der *DSM-Explorer-Hilfe*.

Aktivieren des ENC-Clients

Standardmäßig kopiert der DSM-Installer die Dateien für den ENC-Client auf die Festplatte, aktiviert sie jedoch nicht. Wenn Sie den Client zu einem späteren Zeitpunkt aktivieren möchten, müssen Sie dazu mehrere Schritte ausführen, die vom Hilfsprogramm "encUtilCmd" auf bequeme Weise abgewickelt werden.

Führen Sie zum Aktivieren des Clients die folgenden Befehle aus:

```
//sofern für die Netzwerkumgebung erforderlich
encutilcmd client -proxy_http [proxy_socks] -proxy_host
vollständiger_Name_des_Proxyservers -proxy_port proxy_port_number
        -user Benutzername -password Kennwort

encUtilCmd client -state enabled -server Name_des_Gateway-Servers [-port n]
caf start
```

Hinweis: Wenn der Client aktiviert wird, bewirkt dies, dass CA Message Queuing (CAM) und der Secure Socket Adapter Port Multiplexer (SSA PMUX) neu gestartet werden. Der Grund hierfür ist, dass ENC in diese beiden Komponenten integriert ist und ein Neustart erforderlich ist, damit diese ENC "wahrnehmen".

Bereitstellung in einer ENC-Umgebung

Für die erfolgreiche Bereitstellung von Software in einer ENC-Umgebung, d. h. mit einer zwischengeschalteten Firewall, müssen die folgenden Voraussetzungen erfüllt sein:

- Die Infrastructure Deployment-Komponente von CA ITCM erfordert, dass sowohl der DMPrimer als auch die Datei "dmkeydat.cer " (Bereitstellungszertifikat) auf dem Zielcomputer vorhanden sind.

  Einzelheiten dazu, wie sich dies bewerkstelligen lässt, finden Sie in den Abschnitten Manuelle Installation der Primer-Software für Infrastructure Deployment (siehe Seite 253) und Bereitstellen des Deployment Management-Sicherheitsschlüssels für eine Primer-Installation (siehe Seite 254).

- Die ENC-Client-Komponente muss auf dem Zielcomputer ausgeführt werden und betriebsbereit sein. Die ENC-Client-Komponente wird mit der Basis-Hardware-Inventar-Komponente installiert und betriebsbereit gemacht, indem ihre Konfiguration festgelegt wird.
- Die Optionen "Hostnamen verwenden" und "Kein Anpingen von Ziel während Scan" der Infrastructure Deployment-Richtlinie müssen auf "True" (Wahr) gesetzt sein.
- Die Infrastructure Deployment-Richtlinienoption "Primer immer bereitstellen" muss auf "Falsch" gesetzt sein. Der Grund dafür ist, dass das Ziel in einer ENC-Umgebung wahrscheinlich über eine Firewall verfügt, so dass der Primer nicht wie üblich bereitgestellt werden kann, sondern eine alternative Methode zum Einsatz kommen muss.

ENC-Bereitstellungsszenarios

In diesem Abschnitt werden die Szenarios beschrieben, bei denen es sich voraussichtlich um die am häufigsten vorkommenden Szenarios handelt, bei denen die ENC-Gateway-Funktionalität eingesetzt wird. Sie basieren auf dem Pilotschema, der Niederlassung und dem IT-Outsourcer.

In den Outsourcer-Szenarios haben Unternehmen verschiedener Größe das Management ihrer Desktops und Server an ein auf IT-Management spezialisiertes Unternehmen übertragen. CA IT Client Manager wird für die üblichen technischen Verwaltungsaufgaben eingesetzt, es benötigt jedoch die ENC-Gateway-Funktionalität, um über Firewalls und das Internet hinweg funktionieren zu können. Ein Outsourcing-Unternehmen kann natürlich alle Szenarios gleichzeitig und mehrmals handhaben.

Es sind natürlich auch weitere Szenarios möglich.

Bei jedem Szenario werden die für die Installation und Konfiguration des Systems erforderlichen Schritte sowie die erwarteten Ergebnisse beschrieben.

In den nachfolgenden Abschnitten werden die folgenden ENC-Bereitstellungsszenarios betrachtet:

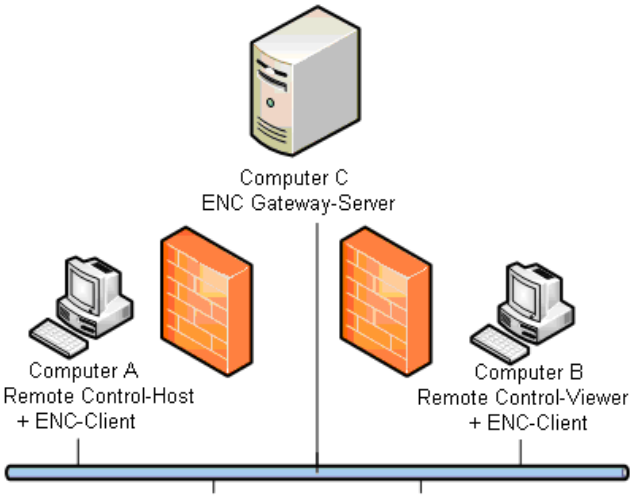
- Szenario 1: Das Pilotschema (siehe Seite 491)
- Szenario 2: Die Niederlassung (siehe Seite 496)
- Szenario 3: Kleines Outsource-Client-Unternehmen (siehe Seite 500)
- Szenario 4: Mittleres Outsource-Client-Unternehmen (siehe Seite 501)
- Szenario 5: Großes Outsource-Client-Unternehmen (siehe Seite 502)

ENC-Bereitstellungsszenario – Das Pilotschema

Dieses Szenario ist voraussichtlich das erste, das ein Unternehmen anwendet, und es soll Erfahrungen mit der Funktionsweise des Systems liefern. Es dient außerdem als einfaches Beispiel zur Erläuterung der Funktionsweise des ENC-Gateways.

Dieses Szenario basiert einfach auf drei Computern. Zwei davon sind Agentencomputer hinter Personal Firewalls von Windows, und beim dritten handelt es sich um einen ENC-Gateway-Server, der die Verbindung ermöglicht.

Die folgende Abbildung zeigt das Layout des Pilotschema-Szenarios:



In diesem Szenario wird auf Computer A ein Remote Control-Host ausgeführt, auf Computer B ein Remote Control-Viewer und auf Computer C ein ENC-Gateway-Server. Computer B kann keine Verbindung zu Computer A herstellen, da er sich hinter einer Firewall befindet. Auf allen Computern werden ENC-Clients ausgeführt, die mit dem ENC-Gateway-Server auf Computer C verbunden sind. Die Verbindung von Computer B zu Computer A wird durch Computer C geschaffen. Das Setup wird nicht durch einen Domänen-Manager verwaltet, um das Szenario so einfach wie möglich zu halten.

Sie können ein kleines ENC-Gateway-Netzwerk einrichten, indem Sie die folgenden Schritte ausführen:

Auf Computer A:

1. Aktivieren Sie die Windows-Firewall.
2. Starten Sie eine benutzerdefinierte Installation von CA ITCM. Wählen Sie "Remote Control" und "Agent".
3. Wenn Sie durch den Installer zur Eingabe der Adresse des Scalability-Servers aufgefordert werden, verwenden Sie den voreingestellten Standardwert. Wenn Sie durch den Installer zur Bestätigung der Angabe aufgefordert werden (da kein Server vorhanden ist), klicken Sie auf "Ja". Dies ermöglicht die Verwendung einer nicht verwalteten Installation.
4. Klicken Sie auf "ENC-Client", um mit der Konfiguration des Clients zu beginnen. Geben Sie die Adresse von Computer C als Serveradresse des Clients ein.
5. Klicken Sie auf "Remote Control", und wählen Sie nur "Hostfunktionen installieren".

6. Wenn die Installation abgeschlossen ist, starten Sie CA ITCM nicht. Führen Sie stattdessen die folgenden Befehle aus:

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/host/managed -pn
   centralizedsecurity -v 0
   ```

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/host/managed -pn standalone -v 1
   ```

7. Starten Sie CA ITCM durch den Befehl "caf start".

Auf Computer B:

1. Aktivieren Sie die Windows-Firewall.
2. Starten Sie eine benutzerdefinierte Installation. Wählen Sie "Remote Control" und "Viewer".
3. Keine Scalability-Server-Angabe (fahren Sie fort wie auf Computer A).
4. Konfigurieren Sie einen ENC-Client auf dieselbe Weise wie auf Computer A.
5. Klicken Sie auf "Remote Control", und wählen Sie nur "Viewer-Funktion installieren".
6. Wenn die Installation abgeschlossen ist, starten Sie CA ITCM nicht. Führen Sie stattdessen den folgenden Befehl aus:

   ```
   ccnfcmda -cmd setparametervalue -ps itrm/rc/viewer/managed -pn managedmode -v
   0
   ```

7. Starten Sie CA ITCM durch den Befehl "caf start".

Auf Computer C:

1. Stellen Sie sicher, dass die Windows-Firewall deaktiviert ist.
2. Starten Sie eine benutzerdefinierte Installation. Löschen Sie alle Produkte. Heben Sie im Dialogfeld der benutzerdefinierten Installation die Auswahl aller Optionen außer "ENC-Gateway" und "Agent" auf.
3. Keine Scalability-Server-Angabe (fahren Sie fort wie auf Computer A und C).
4. Wählen Sie im Dialogfeld zur Konfiguration des ENC-Gateways alle drei Rollen aus: Manager, Server und Router.
5. Starten Sie CA ITCM auf diesem Computer nicht jetzt. Die Sicherheit für den Gateway-Server wurde noch nicht konfiguriert und weist alle Verbindungen von Clients zurück. Zur Konfiguration der ENC-Sicherheit erstellen wir nun beispielhaft eine Textdatei, die eine Regel enthält, die alle Verbindungen zulässt. Die Datei wird anschließend in den gemeinsamen Speicher importiert, damit der Server sie aufnehmen kann.

   Wichtig! Beachten Sie, dass es sich hier nur um ein Beispiel handelt. In einer echten Produktionsumgebung würde man niemals Regeln verwenden, die einen offenen Zugriff erlauben!

6. Erstellen Sie eine Textdatei mit dem Namen "defrules.txt", die den folgenden Text enthält:

```
[authz]
RulesVersion=5

REALM
{Name "ENC" Notes "Der Standardbereich, zu dem jeder gehört"}
end

TimeRange
{Name "Alle Tage" enabled "1" Hours "00:00 - 00:00" Type "normal" Weekdays
"sunday - saturday"}
end

TimeACL
{Name "Richtlinie1" enabled "1" RuleType "allow" Events
"AuthenticatedConnection ManagerRegisterServer ServerRegisterRouter
ManagerRegisterRouter ServerRegisterAgent ManagerRegisterAgent
ManagerNameLookup AgentConnect RouterAgentConnect ManagementAccess" TimeRange
"Alle Tage" SecPrincType "realm" SecPrinc "ENC" SecObj "ENC" SecObjType
"realm"}
end

URIMapping
{URI ".+" enabled "1" Type "pattern" Realm "ENC"}
end

IPAddWhiteList
{IPAddress ".+" enabled "1" Type "pattern"}
end
```

7. Importieren Sie diese Regeldatei wie folgt mit dem Befehl "encUtilCmd":
   `Encutilcmd import -i defrules.txt -fl`

   Der ENC-Gateway-Server besitzt jetzt eine Regel, die alle Verbindungen zulässt.

8. Installieren Sie schließlich ENC-Zertifikate auf allen Computern. Informationen hierzu finden Sie unter Einrichten von Zertifizierungsdiensten zur Verwendung durch ENC-Gateway (siehe Seite 508).

Führen Sie die folgenden Schritte aus, um das Szenario zu testen:

1. Starten Sie auf Computer A und B CA ITCM mit dem Befehl "caf start". Starten Sie Computer C noch nicht, da der Test ohne die ENC-Gateway-Funktionalität durchgeführt werden soll.
2. Starten Sie das Dialogfeld für die Host-Konfiguration, indem Sie es in der Taskleiste auf Computer A auswählen. Wählen Sie die Registerkarte "Benutzer", und stellen Sie sicher, dass der lokale Administrator auf diesem Computer ein Benutzer von Remote Control ist.
3. Starten Sie auf Computer B den Viewer, und versuchen Sie, eine Verbindung herzustellen. Dieser Vorgang müsste durch die Firewall auf Computer A blockiert werden.

4. Starten Sie CA ITCM auf Computer C. Überprüfen Sie nach einigen Minuten, ob sich die ENC-Clients beim ENC-Gateway-Server registriert haben, indem Sie den Befehl "encclient status" ausführen. Daraufhin sollte gemeldet werden, dass sich der Client erfolgreich registriert hat und bereit ist.

5. Wiederholen Sie den Verbindungsversuch. Dieses Mal müsste er erfolgreich sein. Alle Daten werden über Computer C weitergeleitet. Der Befehl "encclient status" sollte melden, dass eine Verbindung über Computer C ausgeführt wird.

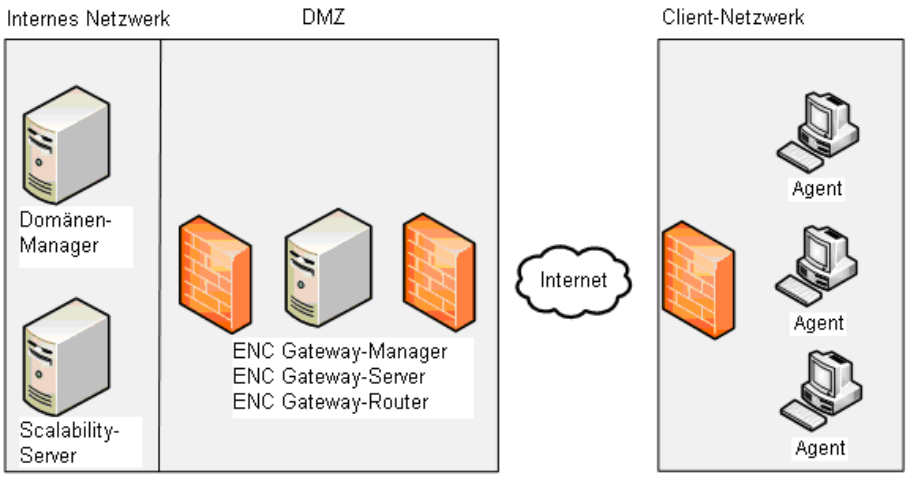
6. Sie können die Regeln anpassen, indem Sie die Datei "defrules.txt" ändern und neu importieren, jedoch unter Verwendung des Befehls "encUtilCmd" mit der Option "-o", um die vorhandenen Regeln zu überschreiben. Auf diese Weise können Sie mit verschiedenen Autorisierungsregeln experimentieren und erhalten so ein Gefühl für das System.

   (Eine detaillierte Beschreibung von "encUtilCmd" und seinen Optionen finden Sie in der *EncUtilCmd-Befehlsreferenz*, die im *CA Bookshelf* in der Kategorie "Referenzhandbücher" zur Verfügung steht.)

ENC-Bereitstellungsszenario – Die Niederlassung

In diesem Szenario unterhält das Mutterunternehmen den Domänen-Manager und den Scalability-Server im Netzwerk der Hauptgeschäftsstelle (internes Netzwerk). Die Niederlassung verfügt über ein LAN, auf dessen Computern DSM-Agenten installiert sind (Client-Netzwerk). Beide Geschäftsstellen sind durch Firewalls geschützt und mit dem Internet verbunden.

Die folgende Abbildung zeigt das Netzwerklayout bei einem Beispiel für ein Niederlassungs-Bereitstellungsszenario:



Bei diesem Szenario wird angenommen, dass auf allen Computern im Netzwerk, einschließlich der ENC-Gateway Server-Computer, mindestens ein DSM-Agent installiert ist.

Die entmilitarisierte Zone (DMZ, Demilitarized Zone) lässt Verbindungen vom internen Netzwerk in diese Zone zu, jedoch nicht darüber hinaus. Computer in der entmilitarisierten Zone können ausgehende Verbindungen zum Internet herstellen, jedoch keine Verbindungen zum internen Netzwerk.

Dies sind die erforderlichen Bereitstellungs- und Konfigurationsschritte bei diesem Szenario:

- Bereitstellen der ENC-Infrastruktur in der Hauptgeschäftsstelle (internes Netzwerk)
- Bereitstellen von DSM-Agenten in der Niederlassung (Client-Netzwerk)
- Konfigurieren der Agenten in der Niederlassung, sodass sie dem Scalability-Server in der Hauptgeschäftsstelle unterstehen

Für das Netzwerk der Hauptgeschäftsstelle gelten die folgenden Aktivitäten:

- Erstellen Sie im Netzwerk der Hauptgeschäftsstelle eine entmilitarisierte Zone, sofern diese nicht bereits vorhanden ist. Dies ist erforderlich, da die ENC-Gateway-Server für die Niederlassung sichtbar sein müssen, von der angenommen wird, dass sie eine Verbindung über das öffentliche Internet herstellt.
- Installieren Sie nach Bedarf einen DSM-Domänen-Manager, einen Scalability-Server, Agenten und ENC-Clients im übergeordneten Netzwerk.
- Installieren Sie einen DSM-Agenten, einen ENC-Client, einen Manager, einen Server und einen Router auf einem Computer, der sich in der entmilitarisierten Zone des Netzwerks der Hauptgeschäftsstelle befindet. Konfigurieren Sie den Agenten so, dass er sich auf dem Scalability-Server im internen Netzwerk registriert.
- Installieren Sie ENC-Zertifikate auf allen ENC-Gateway-sensitiven Computern, wie im Abschnitt Verwaltung von Zertifikaten (siehe Seite 508) beschrieben. Dies umfasst Computer im internen Netzwerk und in der entmilitarisierten Zone. Diese Zertifikate sind für die ENC-Gateway-Authentifizierung erforderlich.
- Installieren Sie ENC-Zertifikate auf den Computern in der entmilitarisierten Zone.
- Starten Sie die ENC-Gateway-Server noch nicht. Zu diesem Zeitpunkt wurden für den ENC-Gateway-Server noch keine Autorisierungsregeln konfiguriert, daher weist er alle Verbindungen zurück. Dies bedeutet, dass die DSM-Infrastruktur in der entmilitarisierten Zone keinen Kontakt zum Domänen-Manager im Netzwerk der Hauptgeschäftsstelle herstellen und daher die Konfigurationsrichtlinie, die die Autorisierungsregeln enthält, nicht empfangen kann.
- Öffnen Sie den DSM-Explorer, und konfigurieren Sie die Sicherheitsrichtlinie, die Sie für ENC benötigen. Konfigurieren Sie den ENC-Gateway mit einer Sicherheitsrichtlinie. Diese muss den Zugriff sowohl für die Computer im Netzwerk der Hauptgeschäftsstelle als auch für die Computer in der Niederlassung regeln. Zu diesem Zeitpunkt kann die Sicherheitsrichtlinie jedoch nicht vom Domänen-Manager aus an die ENC-Gateway-Server gesendet werden, da die folgende catch-22-Situation besteht: Der Computer kann erst dann eine Richtlinie empfangen, wenn er sich beim Domänen-Manager registriert, und er kann sich erst dann registrieren, wenn er eine Richtlinie erhält, die die Autorisierungsregeln definiert, die zulassen, dass der Computer eine Verbindung zum Domänen-Manager herstellt.

- Zur Behebung dieses Problems muss der ENC-Gateway-Server mit Regeln gestartet werden, die ausreichen, um eine Verbindung zum Domänen-Manager zuzulassen. Sobald die Verbindung hergestellt wurde, kann der Domänen-Manager die echte Richtlinie senden, um die Richtlinie für den Neustart zu überschreiben.

  Zuerst muss die echte Richtlinie in die Konfigurationsrichtlinie auf dem Domänen-Manager eingegeben werden. Dies kann mit einer der folgenden beiden Methoden geschehen:

  1. Eine Methode besteht darin, den DSM-Explorer zu öffnen und die Sicherheitsrichtlinie, die Sie für ENC benötigen, mit Hilfe des Konfigurationsrichtlinien-Editors zu konfigurieren. Die GUI verfügt über ein benutzerdefiniertes Dialogfeld, das Sie beim Erstellen der Regeln unterstützt.
  2. Die alternative Methode besteht darin, eine Textdatei mit Ihren Standardregeln zu erstellen und diese mit dem Hilfsprogramm "encUtilCmd" in einem Schritt zu importieren. (Eine detaillierte Beschreibung von "encUtilCmd" und seinen Optionen finden Sie in der *EncUtilCmd-Befehlsreferenz*, die im *CA Bookshelf* in der Kategorie "Referenzhandbücher" zur Verfügung steht.) Beachten Sie, dass "encUtilCmd" auch eine Möglichkeit zur Vorabprüfung der Regeln zur Verfügung stellt.

  Diese Regeln sollten mindestens zulassen, dass die DSM-Infrastruktur im Netzwerk der Hauptgeschäftsstelle Kontakt mit der ENC-Gateway-Infrastruktur in der entmilitarisierten Zone aufnimmt und sich bei ihr registriert.

  Es empfiehlt sich, die Regeln mit der zweiten Methode zu erstellen, da die Regeldatei, die Sie erstellen, dann sowohl auf dem Domänen-Manager als auch auf den ENC-Server-Computern verwendet werden kann. Die GUI kann für spätere Änderungen an der Richtlinie verwendet werden.

  Wenden Sie die Regeln mit Hilfe des Befehls "encUtilCmd importdb" auf den Domänen-Manager an. Dadurch werden die Regeln zur DSM-Konfigurationsdatenbank hinzugefügt. Wenn sie sich dort befinden, können sie über den üblichen Richtlinienmechanismus geliefert werden, sobald die ENC-Server-Computer eine Verbindung herstellen.

  Wenden Sie diese Regeln mit Hilfe des Befehls "encUtilCmd import" auf den ENC-Gateway-Server in der entmilitarisierten Zone an. Dadurch wird der Server mit Autorisierungsregeln gestartet, und es wird zugelassen, dass der Computer den Kontakt zum Domänen-Manager herstellt und sich registriert.

  Starten Sie CA IT Client Manager auf den ENC-Gateway-Servern, damit sie die neuen Regeln annehmen und es ENC-Verbindungen erlauben, fortzufahren.

- Standardmäßig ist die Konfigurationsrichtlinie im Domänen-Manager auf "Lokal verwaltet" gesetzt, um zu verhindern, dass sie versehentlich durch eine leere Richtlinie überschrieben wird. Setzen Sie diesen Wert auf "Zentral verwaltet". Wenn CA IT Client Manager sich erfolgreich registriert, wird die anfängliche Standardregel durch die vom Domänen-Manager gesendete Richtlinie überschrieben.

- Warten Sie 10 Minuten, und überprüfen Sie dann, ob sich die Computer in der entmilitarisierten Zone nun registriert haben und in der GUI angezeigt werden.
- Wenn keine Computer angezeigt werden, sind die Standardregeln möglicherweise nicht korrekt oder die neue Richtlinie hat den Zugriff unterbunden. Dies können Sie dem NT-Anwendungsereignisprotokoll auf den ENC-Gateway-Servern entnehmen.

Für die Niederlassung gelten die folgenden Aktivitäten:

- Installieren Sie die erforderlichen DSM-Agenten auf jedem Computer im Netzwerk der Niederlassung. Die ENC-Gateway-Funktionalität wird standardmäßig installiert, sie muss jedoch konfiguriert werden. Konfigurieren Sie die Clients so, dass sie sich auf dem ENC-Gateway-Server im Netzwerk der entmilitarisierten Zone der Hauptgeschäftsstelle registrieren. Da das ENC-Gateway zwischen der Hauptgeschäftsstelle und der Niederlassung noch nicht funktioniert, kann die DSM-Bereitstellung nicht verwendet werden. Stattdessen kann die Installation mit einer von mehreren Methoden ausgeführt werden, die davon abhängen, wie viele Computer betroffen sind, z. B.:
  - Manuelle Installation von DVD, wenn nur wenige Computer betroffen sind
  - Installation eines Pakets bei der Benutzeranmeldung von einem NT-Domänen-Anmeldeskript aus.
  - Installation eines temporären Domänen-Managers und Scalability-Servers innerhalb des Netzwerks der Niederlassung. Dies kann mit Hilfe eines realen oder virtuellen Computers erfolgen, der an die Niederlassung gesendet wird. Verwenden Sie die Bereitstellungsfunktion von CA IT Client Manager, um das Agentenpaket zu versenden. Sobald die Bereitstellung abgeschlossen ist und sich alle Agenten beim Domänen-Manager in der Hauptgeschäftsstelle registrieren, wird der temporäre Domänen-Manager in der Niederlassung entfernt.
- Überprüfen Sie, ob sich die Computer in der Niederlassung registrieren, indem Sie die Gruppe "Alle Computer" in der GUI in der Hauptgeschäftsstelle markieren.
- Führen Sie die üblichen in Ihrem Unternehmen eingesetzten Validierungstests durch, um sicherzustellen, dass CA IT Client Manager voll funktionsfähig ist.

ENC-Bereitstellungsszenario – Kleines Outsourcing-Client-Unternehmen

Das Szenario für ein kleines Unternehmen ist dem für eine Niederlassung sehr ähnlich, abgesehen davon, dass eine höhere Sicherheit erforderlich ist. Da der Outsourcer möglicherweise für viele verschiedene Unternehmen tätig ist, ist eine stärkere Kontrolle der zugelassenen Vernetzung zwischen den Knoten in den einzelnen Unternehmensnetzwerken erforderlich. Außerdem muss der Zugriff von einem Outsource-Client auf einen anderen gesichert werden. Normalerweise wird nicht zugelassen, dass ein Client die Computer in einem anderen Client sieht. Dies wird durch die Unterstützung für Bereiche in der ENC-Gateway-Autorisierung gehandhabt.

Die Computer in dem Outsourcing-Unternehmen müssen eine Verbindung zu den Computern des Clients herstellen können. Dies erfordert, dass der Outsourcer-ENC-Gateway-Manager mit Autorisierungsregeln konfiguriert wird, die Folgendes zulassen:

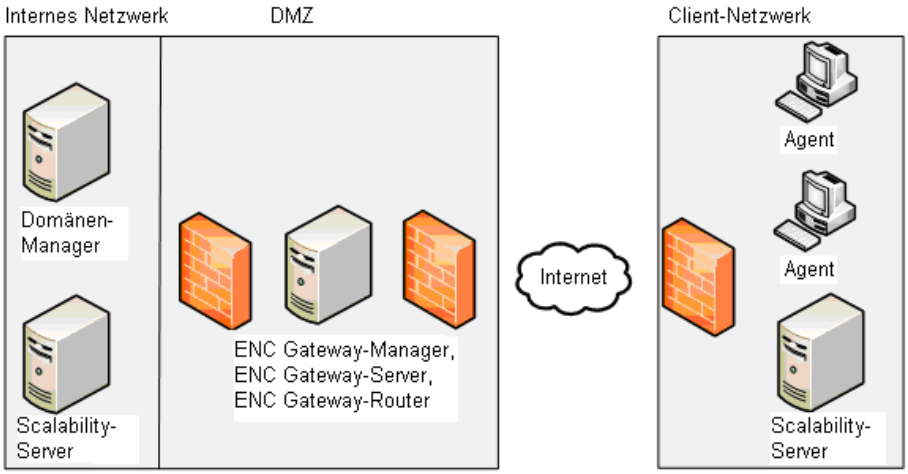
- Die Registrierung von Computern im Client-Netzwerk aus.
- Verbindungen von Computern im Client-Netzwerk zu Computern im Outsourcer-Netzwerk und umgekehrt.
- Verbindungen zwischen verschiedenen Client-Bereichen werden verweigert.

Dies ähnelt dem Konfigurieren und Einrichten von CA ITCM, die Sicherheitsbereichsverwaltung muss jedoch auch für die Behandlung der Sicherheitsanforderungen konfiguriert werden (siehe Kapitel "CA ITCM-Sicherheitsfunktionen" (siehe Seite 403)).

ENC-Bereitstellungsszenario – Mittleres Outsourcing-Client-Unternehmen

In diesem Szenario verfügt der Client über eine ausreichende Anzahl an Computern, um einen eigenen Scalability-Server zu gewährleisten.

Die folgende Abbildung zeigt das Netzwerklayout bei einem Beispiel für ein Bereitstellungsszenario für ein mittleres Outsourcing-Client-Unternehmen:



Die Agenten im Client-Netzwerk registrieren sich dort auf dem Scalability-Server. Der Scalability-Server stellt über eine ENC-Gateway-Verbindung eine Verbindung zum Domänen-Manager im Outsourcer-Netzwerk her. Die Bereitstellungsschritte sind dem Szenario für ein kleines Unternehmen sehr ähnlich, mit Ausnahme der Agentenkonfiguration. In diesem Szenario sind die DSM-Agenten so konfiguriert, dass sie sich auf dem unternehmensinternen Scalability-Server registrieren.

In diesem Szenario mit einem mittelgroßen Outsourcer befindet sich ENC in der Regel nicht auf den Endpunkt-Computern. In diesem Fall bedeutet dies, dass direkte Verbindungen nur dann funktionieren, wenn ENC auf den Endpunkt-Computern konfiguriert ist und ausgeführt wird. Direkte Verbindungen werden für die folgende Kommunikation verwendet:

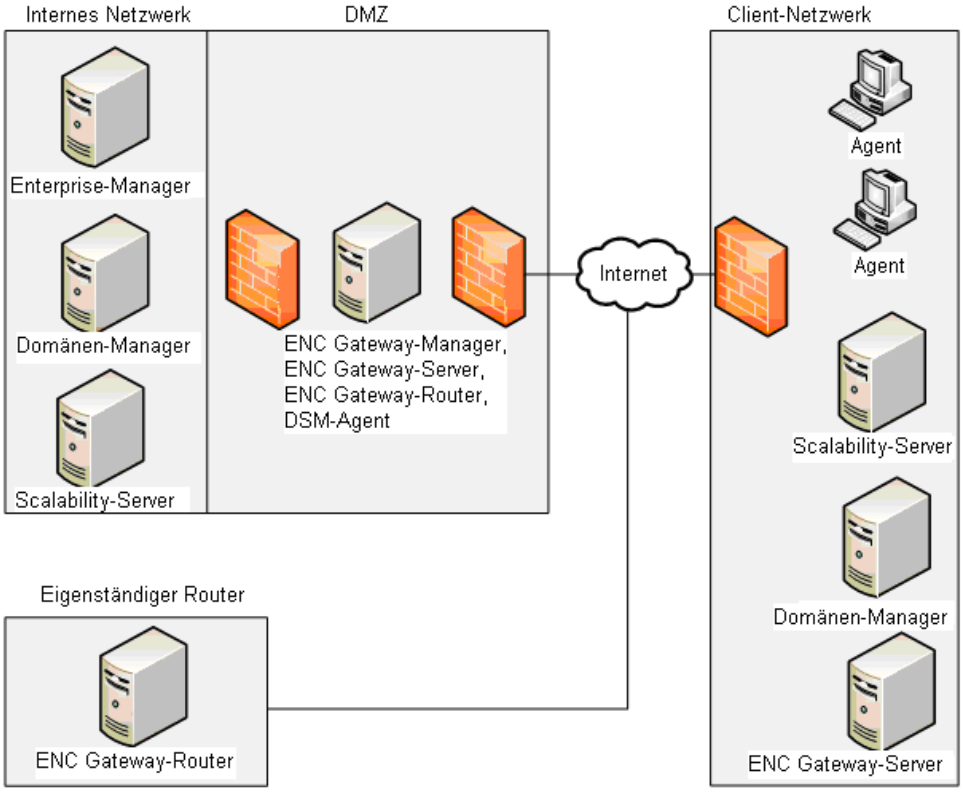
- Remote Control-Host – Verbindung anzeigen
- Sofortdiagnose von DSM-Explorer zum Agenten
- Softwarekatalog vom Agenten zum Manager
- DTS-Benachrichtigungen

ENC-Bereitstellungsszenario – Großes Outsourcing-Client-Unternehmen

In diesem Szenario ist das Unternehmen so groß, dass es über einen eigenen Domänen-Manager sowie mehrere Scalability-Server und einen ENC-Gateway-Server verfügt.

Das Outsourcing-Unternehmen unterhält einen Enterprise-Manager, der mit dem Domänen-Manager des Clients verknüpft werden soll.

Die folgende Abbildung zeigt das Netzwerklayout bei einem ENC-Gateway-Bereitstellungsszenario für ein großes Outsourcing-Client-Unternehmen:



Sobald der Client-Domänen-Manager installiert ist, kann er dazu verwendet werden, DSM-Agenten wie üblich innerhalb des Clients bereitzustellen.

Die Richtlinie kann mit Hilfe des Domänen-Managers des Clients lokal konfiguriert werden, um zuzulassen, dass der Client-ENC-Gateway-Server ENC-Verbindungen von den Client-Computern akzeptiert.

Der Enterprise-Manager repliziert seine Datenbank auf den Domänen-Manager, indem er den Datenbank-Provider selbst verwendet. Dies ist über eine ENC-Gateway-Verbindung nicht möglich. Damit dies funktioniert, müssen die Firewalls so konfiguriert sein, wie in der bestehenden veröffentlichten Best Practice von Microsoft oder Oracle beschrieben.

Die Computer in dem Outsourcing-Unternehmen müssen eine Verbindung zu den Computern des Clients herstellen können. Dies erfordert, dass der Outsourcer-ENC-Gateway-Manager mit Autorisierungsregeln konfiguriert wird, die Folgendes zulassen:

- Verbindungen vom ENC-Gateway-Server des Clients
- Die Registrierung von Computern im Client-Netzwerk aus
- Verbindungen von Computern im Client-Netzwerk zu Computern im Outsourcer-Netzwerk und umgekehrt

Eigenständige ENC-Gateway-Router

Es können auch zusätzliche ENC-Gateway-Router bereitgestellt werden, um Robustheit oder Skalierbarkeit zu erzielen. Diese ENC-Gateway-Router können an einem anderen Ort im Internet oder in Niederlassungen installiert werden.

Dies sind die Bereitstellungsschritte für eigenständige ENC-Gateway-Router:

- Installieren Sie einen DSM-Agenten und einen ENC-Gateway-Router, und konfigurieren Sie ihn so, dass er sich auf dem ENC-Gateway-Server in der Geschäftsstelle des Outsourcers registriert. Der Router kann natürlich so konfiguriert werden, dass er sich auf einem beliebigen anderen geeigneten ENC-Gateway-Server registriert.
- Fügen Sie auf dem Domänen-Manager geeignete Autorisierungsregeln zu der Richtlinie hinzu, die für den Computer des eigenständigen Routers verwendet werden soll. Die Regeln müssen zulassen, dass der Router in dem Bereich, in dem er sich befindet, eine Verbindung herstellen und sich registrieren kann.
- Installieren Sie ein geeignetes Zertifikat auf dem Router-Computer.
- Starten Sie CA ITCM auf dem Router-Computer. Der Router sollte sich dann beim ENC-Gateway-Server registrieren. Überprüfen Sie dies anhand des Ereignisprotokolls.

  Hinweis: Damit diese Ereignisse sichtbar sind, müssen Sie den Konfigurationsparameter "itrm/common/enc/audit/enabled" auf 1 setzen. In der Konfigurationsrichtlinie wird dies als "Alle aktivieren" angegeben. Dies ermöglicht das Auditing aller ENC-Ereignisse. Dadurch können Sie die Aktivität im ENC-System genauer sehen. Standardmäßig sind nur die Ereignisse aus der Kategorie "Fehler" aktiviert. Wenn Sie das normale Auditing wiederherstellen möchten, setzen Sie den Konfigurationsparameter auf 2 ("Aktiviert nach Kategorie").
- Sobald sich der ENC-Client auf dem Router-Computer registriert, kann die CA ITCM-Infrastruktur die Richtlinie akzeptieren und daher Autorisierungsregeln für den Router installieren. Sobald der Router die Autorisierungsregeln aufgenommen hat, kann er als Router für das Verbinden von anderen Computern im ENC-Gateway-Netzwerk fungieren.

Eigenständige ENC-Gateway-Server

Für eigenständige ENC-Gateway-Server gelten ähnliche Überlegungen wie für eigenständige ENC-Gateway-Router. Der Unterschied besteht darin, dass es sich bei den Autorisierungsregeln um die Regeln handelt, die für eine Serverrolle geeignet sind, d. h., sie lassen die Vorgänge zu, die ein Gateway-Server ausführen kann, und nicht diejenigen, die ein Gateway-Router ausführen kann.

Internet-Proxy-Unterstützung

Wenn der Pfad von einem ENC-Client zu einem ENC-Gateway-Server durch einen Internet-Proxy blockiert ist, muss der Client so konfiguriert werden, dass die Verbindung über den entsprechenden Proxy hergestellt wird. Das ENC-Gateway unterstützt SOCKS4-, SOCKS5- und HTTP-Proxys. Die Authentifizierung kann durch einen expliziten Benutzernamen und das dazugehörige Kennwort konfiguriert werden oder durch eine Nachahmung des angemeldeten Benutzers. Der Client kann auch aktuelle Internet Explorer-Einstellungen verwenden, um den Proxy zu suchen.

Die Eigenschaften, die festgelegt werden sollen, befinden sich im Richtlinienknoten 'common components/enc/client'.

Wenn Sie einen SOCKS-Proxy konfigurieren möchten, legen Sie die folgenden Parameter fest:

- SocksProxyAddress und SocksProxyPort zur Identifizierung des Proxy-Computers
- SocksProxyAuthType, um den zu verwendenden Authentifizierungstyp zu definieren ("Standard" oder "Sicher")
- SocksProxyImpersonate: Ermöglicht dem Client, die Anmeldeinformationen des angemeldeten Benutzers zu verwenden. Dies bedeutet natürlich, dass der Client nur dann eine Verbindung herstellen kann, wenn ein Benutzer angemeldet ist.
- SocksProxyUsername und SocksProxyPassword, wenn Sie für die Authentifizierung mit dem Proxy explizite Anmeldeinformationen verwenden möchten
- SocksProxyDiscovery, wenn der ENC-Client den Proxy automatisch mit Hilfe von IE-Einstellungen suchen soll. In diesem Fall ist in der Regel SocksProxyImpersonate festgelegt.

Wenn Sie einen HTTP-Proxy konfigurieren möchten, legen Sie dieselben Parameter fest, abgesehen davon, dass in den Parameternamen "Socks" durch "HTTP" ersetzt wird.

Hinweis: Die Proxykonfiguration kann auch mit dem Hilfsprogramm "encUtilCmd" festgelegt werden. Dies ist hilfreich, wenn der fragliche Computer durch die Firewall von der verwalteten Richtlinie getrennt ist, aber natürlich zum Herstellen einer Verbindung Richtlinieneinstellungen benötigt.

Einschränkungen für die Verwendung von CA ITCM über ein ENC-Gateway

Wenn CA IT Client Manager (CA ITCM) über eine ENC-Gateway-Verbindung verwendet wird, bestehen verschiedene Funktionseinschränkungen. Zu diesen Einschränkungen gehört Folgendes:

- Wake-on-LAN (WOL) funktioniert über den ENC-Gateway nicht, da das ENC-Gateway nur TCP-Verbindungen unterstützt, WOL jedoch UDP verwendet.
- Manche Funktionen der Sofortdiagnose funktionieren nicht, da sie von Nicht-ENC-Gateway-sensitiven Komponenten abhängig sind, die mit dem Betriebssystem zur Verfügung gestellt werden, z. B. FTP.
- Der Dienst-Locator funktioniert nicht, da er UDP verwendet.
- Der Reporter funktioniert nicht, da er direkt auf die MDB zugreift.
- Es kann bis zu 10 Minuten dauern, bis Software Delivery (SD)-Jobs, die über das ENC-Gateway ausgeführt werden, ausgelöst werden. Dies liegt daran, dass SD versucht, die IP-Adresse des Ziels bei dessen Registrierung zu verwenden, was jedoch fehlschlägt, weil IP-Adressen nicht über verschiedene Netzwerke gültig sind. Der SD-Scalability-Server versucht alle 10 Minuten erneut, den Job auszuführen, und wechselt dabei zwischen dem vollständigen Namen und der IP-Adresse des Ziels. Der vollständige Name funktioniert mit dem ENC-Gateway, da er von ENC-Gateway-fähigen Computern verwendet wird, um diese eindeutig zu identifizieren.
- Einige Komponenten innerhalb von CA ITCM verwenden clientseitige SQL Server- oder Oracle-Komponenten zum Herstellen von direkten Management-Datenbank (MDB)-Verbindungen. Diese Verbindungen sind nicht ENC-fähig. Wenn diese Verbindungen durch Firewalls hindurch verlaufen, sollten Sie daher die empfohlene Methode von Microsoft oder Oracle verwenden, um die Firewall zu durchqueren.

  In der folgenden Liste finden Sie Details zu Szenarios und DSM-Komponenten, bei denen ein direkter Zugriff auf die MDB erfolgt. Außerdem sind die spezifischen clientseitigen Komponenten angegeben, die für SQL Server und Oracle verwendet werden:

  - **Domänen-Manager zum und vom Enterprise-Manager**

    Die MDB-Replizierung zwischen dem Domänen-Manager und dem Enterprise-Manager verwendet direkte Verbindungen und kopiert große Datenmengen ("bulk copy").

    Clientseitige Komponenten:

    Für SQL Server: SQL Native Client und bcp Utility

    Für Oracle: OCI API und SQL*Loader

- **Engine zum Domänen-Manager und zum Enterprise-Manager**

  Die Engine stellt bei der Kommunikation mit dem Domänen-Manager und dem Enterprise-Manager direkte Datenbankverbindungen her.

  Clientseitige Komponenten:

  Für SQL Server: SQL Native Client und bcp Utility

  Für Oracle: OCI API und SQL*Loader

- **Reporter zum Domänen-Manager oder zum Enterprise-Manager**

  Der Reporter stellt zum Generieren von Berichten direkte Datenbankverbindungen her.

  Clientseitige Komponenten:

  Für SQL Server: SQL Native Client und bcp Utility

  Für Oracle: OCI API und SQL*Loader

- **Webkonsole zum Domänen-Manager oder zum Enterprise-Manager**

  Die Webkonsolen-Komponente stellt eine JDBC-Verbindung zur Datenbank her.

  Clientseitige Komponenten:

  Für SQL Server: JDBC

  Für Oracle: JDBC

- **Hilfsprogramm für den Import/Export von Inhalten**

  Das Hilfsprogramm für den Import/Export von Inhalten stellt bei der Synchronisation von DSM-Daten mit einer Remote-Oracle- oder SQL Server-MDB direkte Datenbankverbindungen her.

  Clientseitige Komponenten:

  Für SQL Server: SQL Native Client und bcp Utility

  Für Oracle: OCI API und SQL*Loader

Verwenden des Hilfsprogramms "encUtilCmd"

Das Hilfsprogramm "encUtilCmd" dient zur Implementierung verschiedener ENC-Gateway-Hilfsprogrammfunktionen. In diesem Abschnitt wird jedoch nur eine Verwendung von "encUtilCmd" behandelt.

Eine detaillierte Beschreibung des Befehls "encUtilCmd" und seiner Optionen finden Sie in der *EncUtilCmd-Befehlsreferenz*, die im CA Bookshelf in der Kategorie "Referenzhandbücher" zur Verfügung steht.

Mit dem Hilfsprogramm "encUtilCmd" lässt sich zusätzlich zu anderen Funktionen die ENC-Gateway-Sicherheit konfigurieren.

In diesem Verwendungsbeispiel wird ein Problem betrachtet, das nach der Installation eines Scalability-Servers auftritt, der gesperrt ist. Der Domänen-Manager kann keine direkte Verbindung zum Scalability-Server herstellen, da dies durch eine Firewall verhindert wird. Daher kann diese Methode nicht verwendet werden, um die Richtlinie auf den Scalability-Server zu verteilen. Der Domänen-Manager kann das ENC-Gateway nicht verwenden, um Kontakt zum Scalability-Server herzustellen, da der Scalability-Server alle Verbindungsversuche zurückweist. Welche Verbindungen zum Scalability-Server zugelassen werden, wird durch eben diese Richtlinie definiert.

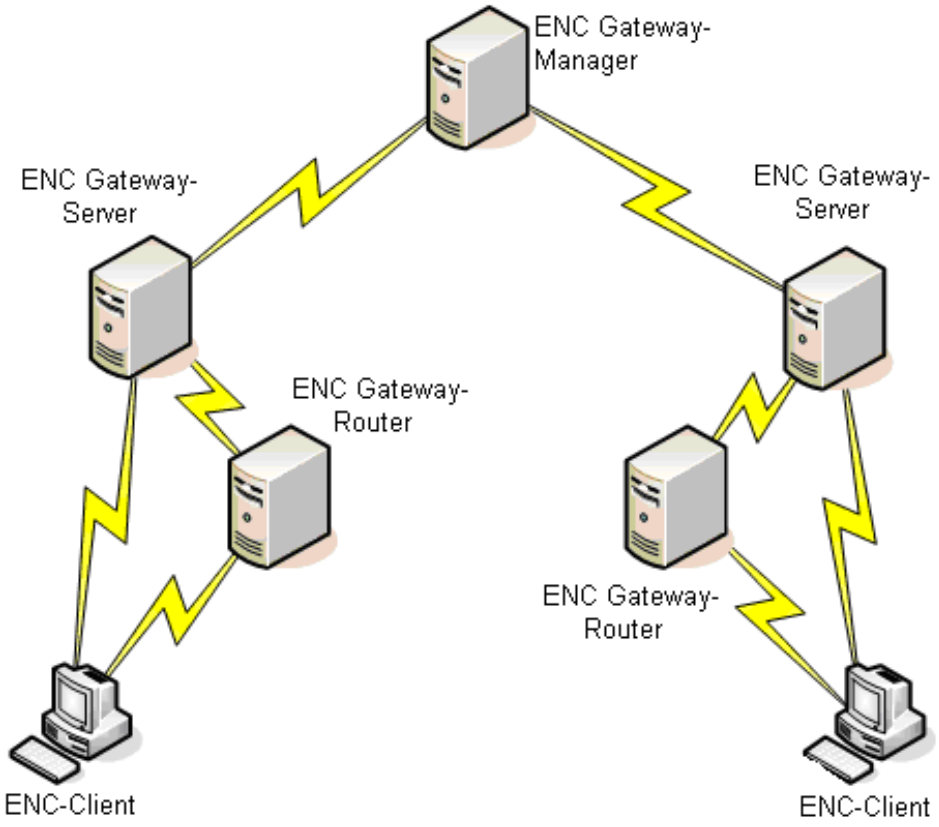
Zur Lösung dieses Problems können Sie Regeln in einer Textdatei definieren und diese Datei mit dem Befehl "encUtilCmd" auf dem ENC-Gateway-Server importieren.

Verwaltung von Zertifikaten

In der Extended Network Connectivity (ENC)-Infrastruktur wird die gesamte Kommunikation zwischen Knoten mit dem standardmäßigen TLS-Protokoll (Transport Layer Security) gesichert. Dieses Protokoll bietet Vertraulichkeit, Integrität und gegenseitige Authentifizierung.

Der Authentifizierungsanteil des TLS-Protokolls wird durch die Verwendung von digitalen Zertifikaten und der Kryptographie mit öffentlichen und privaten Schlüsseln bereitgestellt. Die Vertraulichkeit wird durch die Kryptographie mit symmetrischen Schlüsseln gewährleistet.

Die folgende Abbildung zeigt Knotenverbindungen zwischen den ENC-Komponenten in einer ENC-Infrastruktur:



Alle Verbindungen zwischen Knoten in der ENC-Infrastruktur sind durch die TLS-Authentifizierung geschützt. Die Authentifizierung erfolgt immer gegenseitig: Der Initiator einer Verbindung authentifiziert sich beim Responder, und der Responder authentifiziert sich beim Initiator. Dies ermöglicht der ENC-Infrastruktur, Computer zu validieren, die eine Verbindung zu ihr herstellen, und verschafft den ENC-Clients Sicherheit hinsichtlich des Ziels ihrer Verbindung.

X.509-Zertifikate

Extended Network Connectivity (ENC) verwendet für die Authentifizierung digitale X.509-Zertifikate der Version 3. Das verwendete Zertifikatsprofil ist das der Implementierung RFC 3280 der Arbeitsgruppe IETF PKIX.

Die Zertifikate und die dazugehörigen privaten Schlüssel werden über den Microsoft-Zertifikatsspeicher abgerufen. Die Zertifikate sollten eine zusätzliche Schlüsselverwendungserweiterung besitzen, die abhängig von der Anwendung, die sie verwendet, für die Server-Authentifizierung (1.3.6.1.5.5.7.3.1) oder die Client-Authentifizierung (1.3.6.1.5.5.7.3.2) markiert ist.

Eine private CA ITCM-Erweiterung für die zusätzliche Schlüsselverwendungs-Zertifikatserweiterung kann zur Unterstützung der Zertifikatssuche (1.3.6.1.4.1.791.2.10.8.3) verwendet werden. Diese Objekt-ID (OID) ist eine private ID von CA Technologies und eine interne ID der CA-OID-Baumstruktur.

Für die RSA-Schlüsselgröße, die für das Zertifikatsschlüsselpaar verwendet wird, bestehen keine ENC-Beschränkungen. Bei der verwendeten Schlüsselgröße handelt es sich um eine unternehmensspezifische Entscheidung, es wird jedoch eine Größe von mindestens 1024 Bit empfohlen.

Zertifikatsverwaltung mit einer PKI-Infrastruktur

Das Erstellen und Verteilen von Zertifikaten kann ein schwieriger Prozess sein. Daher empfiehlt sich die Verwendung einer Public Key Infrastructure (PKI) zur Automatisierung und Erweiterung dieses Prozesses.

Zertifikatsanforderungen

Das ENC-Gateway verwendet X.509 v3-Zertifikate, die zur Verwendung durch das standardmäßige Sicherheitsprotokoll TLS 1.0 (SSL 3.1) ausgegeben werden. Das ENC-Gateway kann standardmäßige TLS-Zertifikate verwenden, es unterstützt jedoch auch eine zusätzliche Schlüsselverwendungserweiterung, um dem ENC-Subsystem zu ermöglichen, Zertifikate zu identifizieren, die hauptsächlich für die Verwendung durch das ENC-Gateway vorgesehen sind.

Das ENC-Gateway sucht nach den besten Zertifikaten, die er für seine Identität laden kann. Beim ersten Passthrough sucht es nach gültigen Zertifikaten (mit den dazugehörigen privaten Schlüsseln), die mit der CA-ENC-Verwendungserweiterung (siehe (1) in der folgenden Tabelle) sowie jeweils (4) mit der TLS-Verwendungserweiterung für die Client-Authentifizierung (2) oder die Server-Authentifizierung (3) markiert sind.

Die folgende Tabelle gibt zusätzliche Details zu den im vorausgehenden Absatz mit (1) bis (4) gekennzeichneten Begriffen an:

Markierung	Informationen
(1)	CA Technologies hat intern eine Objekt-ID (OID) reserviert, die in X.509 v3-Zertifikaten als erweiterte Schlüsselverwendungs-ID verwendet werden soll (siehe RFC2459 Abschnitt 4.2.1.13). Diese OID gibt an, dass das Zertifikat zur Verwendung durch das ENC-Sicherheitssubsystem bestimmt ist. ■ Die Objekt-ID ist "1.3.6.1.4.1.791.2.10.8.3" ■ Das Objekt-ID-Tag ist "OID_PKIX_KP_CA_CMS_ENC_TLS_AUTH" ■ Die Verwendungserweiterung kann als kritisch oder nicht kritisch markiert werden. ■ Die CA Technologies-Basis-OID ist "1.3.6.1.4.1.791". Diese ist bei IANA registriert.
(2)	Die OID für die TLS-Client-Authentifizierung ist "1.3.6.1.5.5.7.3.2"
(3)	Die OID für die TLS-Server-Authentifizierung ist "1.3.6.1.5.5.7.3.1"
(4)	Für ENC-Gateway-Knoten, die sowohl als Client als auch als Server fungieren (Router und Gateway-Server), kann das Sicherheitssubsystem entweder ein einziges Zertifikat verwenden, das für die Client- und Server-Authentifizierung markiert ist, oder einzelne Zertifikate, die jeweils nur für die Client-Authentifizierung bzw. nur für die Server-Authentifizierung markiert sind.

Wenn das ENC-Gateway keine geeigneten Zertifikate findet, wiederholt es die Suche ohne die Anforderung der CA-ENC-Verwendungserweiterung.

Wenn Sie Zertifikate zur Verwendung durch das ENC-Gateway erstellen, wird empfohlen, dass Sie die CA-OID für die zusätzliche Schlüsselverwendung zu den Zertifikaten hinzufügen. Das ENC-Gateway funktioniert jedoch auch ohne sie.

Die CA Technologies-Objekt-ID für die private Authentifizierung

Eine private CA ITCM-Erweiterung für die zusätzliche Schlüsselverwendungs-Zertifikatserweiterung kann zur Unterstützung der Zertifikatssuche (1.3.6.1.4.1.791.2.10.8.3) verwendet werden.

Diese Objekt-ID (OID) ist eine private ID von CA Technologies und eine interne ID der CA Technologies-OID-Baumstruktur.

Kapitel 13: Integration in CA Service Desk Manager

Durch die Integration von CA IT Client Manager in CA Service Desk Manager wird CA IT Client Manager zu einer Service-Aware-Anwendung, d. h., dass CA IT Client Manager bei bestimmten Ereignissen seiner verwalteten Assets ausgelöst werden und Tickets in CA Service Desk Manager erstellen kann.

Die Ticketerstellung und der Arbeitsablauf in CA Service Desk Manager werden von der Service-Aware-Richtlinie gesteuert, die eine Liste mit Problemtypen enthält. CA IT Client Manager verwendet Problemtypen zum Kategorisieren des Problems und zum Behandeln des Tickets, das erstellt werden soll.

CA IT Client Manager und CA Service Desk Manager bieten grafische Benutzeroberflächen, die einen kontextabhängigen Start von beiden für die Integration zulassen.

Dieses Kapitel enthält Informationen zum Setup und zur Konfiguration des Systems sowie zu den Sicherheits- und Authentifizierungsaspekten. Die Konfigurationshinweise gelten für DSM-Domänen- und Enterprise-Manager.

Weitere Informationen zu CA Service Desk Manager, z. B. zu Problemtypen, finden Sie in der CA Service Desk Manager-Dokumentation.

Dieses Kapitel enthält folgende Themen:

Service-Aware-Richtlinie (siehe Seite 514)
Ticket-Behandlung (siehe Seite 515)
Erkannte Assets mit eigenen Assets verknüpfen (siehe Seite 515)
Kontextabhängiger Start zwischen CA ITCM und CA Service Desk Manager (siehe Seite 516)
Kontextabhängiger Start von CA Service Desk Manager zu CA ITCM (siehe Seite 519)
Einrichten von CA Service Desk Manager und CA ITCM (siehe Seite 520)
Voraussetzung für einen Start von CA Service Desk Manager innerhalb des Kontextes (siehe Seite 520)
Voraussetzungen für die CA Service Desk Manager-Integration in mehreren Engines (siehe Seite 521)
Voraussetzungen für die CA Service Desk Manager-Integration im Enterprise-Manager (siehe Seite 521)
Informationen zur CA ITCM- und CA Service Desk Manager-Integration (siehe Seite 521)
Sichere Anmeldung beim CA Service Desk Manager-Webdienst (siehe Seite 522)
Einstellungen in der Konfigurationsrichtlinie (siehe Seite 526)

Service-Aware-Richtlinie

Für die Integration von CA ITCM in CA Service Desk Manager wird eine Service-Aware-Richtlinie mit dem Namen "ManagedAssetEvents" festgelegt. Die Service-Aware-Richtlinie wird automatisch während der Installation von CA Service Desk Manager installiert. CA ITCM verwendet beim Erstellen von Tickets die Problemtypen in dieser Richtlinie.

Im Folgenden werden die Hauptparameter der Service-Aware-Richtlinie dargestellt:

Angezeigter Name:

Ereignisse verwalteter Assets

Code:

MANAGED_ASSET_EVENTS

Beschreibung:

Die Service-Aware-Richtlinie wird zum Verarbeiten von Tickets verwendet, die über die Webdienste von den verwalteten Assets ausgelöst werden.

Außer den Standard-Problemtypen von CA Service Desk Manager enthält die Service-Aware-Richtlinie die im Folgenden aufgeführten Problemtypen. CA Service Desk Manager-Administratoren können diese Problemtypen ändern oder die Liste um ihre eigenen Problemtypen erweitern.

Anzeigename des Problemtyps	Code des Problemtyps	Beschreibung des Problemtyps	Priorität (5 ist die höchste)
Asset-ereignisbasierte Richtlinie hoch	ASSET_EVENT_ POLICY_H	Ein verwaltetes Asset fand eine ereignisbasierte Richtlinienverletzung mit hoher Priorität.	4
Asset-ereignisbasierte Richtlinie mittel	ASSET_EVENT_ POLICY_M	Ein verwaltetes Asset fand eine ereignisbasierte Richtlinienverletzung mit mittlerer Priorität.	3
Asset-ereignisbasierte Richtlinie hoch	ASSET_QUERY_ POLICY_H	Ein verwaltetes Asset fand eine abfragebasierte Richtlinienverletzung mit hoher Priorität.	4
Asset-ereignisbasierte Richtlinie mittel	ASSET_QUERY_ POLICY_M	Ein verwaltetes Asset fand eine abfragebasierte Richtlinienverletzung mit mittlerer Priorität.	3

Anzeigename des Problemtyps	Code des Problemtyps	Beschreibung des Problemtyps	Priorität (5 ist die höchste)
Fehlschlagen Softwareverteilung hoch	SW_DISTR_FAIL _H	Ein Software Delivery-Job fand einen Fehler mit hoher Priorität.	4
Fehlschlagen Softwareverteilung mittel	SW_DISTR_FAIL _M	Ein Software Delivery-Job fand einen Fehler mit mittlerer Priorität.	3
Fehlschlagen Softwareverteilung niedrig	SW_DISTR_FAIL _L	Ein Software Delivery-Job fand einen Fehler mit niedriger Priorität.	2

Ticket-Behandlung

Tickets können auf Domänen- und auf Enterprise-Ebene erstellt werden. Durch die folgenden Ereignisse kann ein Ticket erstellt werden:

- Es wird eine Richtlinienverletzung gefunden.
- Ein Software Delivery-Job schlägt fehl.
- Ein Administrator erstellt ein Ticket interaktiv über ein Popup-Menü im Kontext eines Computers.

Um zu vermeiden, dass ein Übermaß an Tickets auftritt, kann das Erstellen neuer Tickets mit folgenden Regeln eingeschränkt werden:

- Für jede Richtlinie wird nur ein Ticket erstellt. Ein Ticket wird neu erstellt, wenn die erste Richtlinienverletzung auftritt. Für jede folgende Verletzung der gleichen Richtlinie wird an das Ticket ein Protokoll angehängt.
- Für jeden Softwarejob wird nur ein Ticket erstellt. Ein Ticket wird neu erstellt, wenn der erste Fehlschlag des Softwarejobs auftritt. Für jeden folgenden Fehlschlag des gleichen Softwarejobs wird an das Ticket ein Protokoll angehängt.

Weitere Informationen zur Ticket-Behandlung finden Sie in der CA Service Desk Manager-Dokumentation

Erkannte Assets mit eigenen Assets verknüpfen

CA ITCM erstellt Tickets im Kontext der erkannten Assets, z. B. der Computer oder Benutzer. Wenn ein Ticket erstellt wird, wird einem eigenen Asset ein erkanntes Asset zugeordnet, das in CA Service Desk Manager bekannt ist. Damit können CA Service Desk Manager-Administratoren navigieren und Berichte zu Beziehungen und eigenen Assets erstellen.

Kontextabhängiger Start zwischen CA ITCM und CA Service Desk Manager

Die folgende Tabelle enthält eine Übersicht der unterstützten kontextabhängigen Starts zwischen dem DSM-Explorer oder der DSM-Webkonsole und der CA Service Desk Manager-Web-GUI.

Von:	An	Im Kontext von	Kontext
Explorer/Webkonsole	CA Service Desk Manager-Web-GUI	Software-Job	Ticket, das bei Fehlschlagen des Jobs erstellt wird
Explorer/Webkonsole	CA Service Desk Manager-Web-GUI	Asset-Richtlinie	Ticket, das bei Verletzung einer Richtlinie erstellt wird
CA Service Desk Manager-Web-GUI	Explorer/Webkonsole	Ticket-Detail	Software-Job
CA Service Desk Manager-Web-GUI	Explorer/Webkonsole	Ticket-Detail	Asset-Richtlinie

Kontextabhängiger Start von CA ITCM zu CA Service Desk Manager

CA ITCM bietet Benutzeroberflächen, mit denen Sie CA Service Desk Manager starten können im Kontext von:

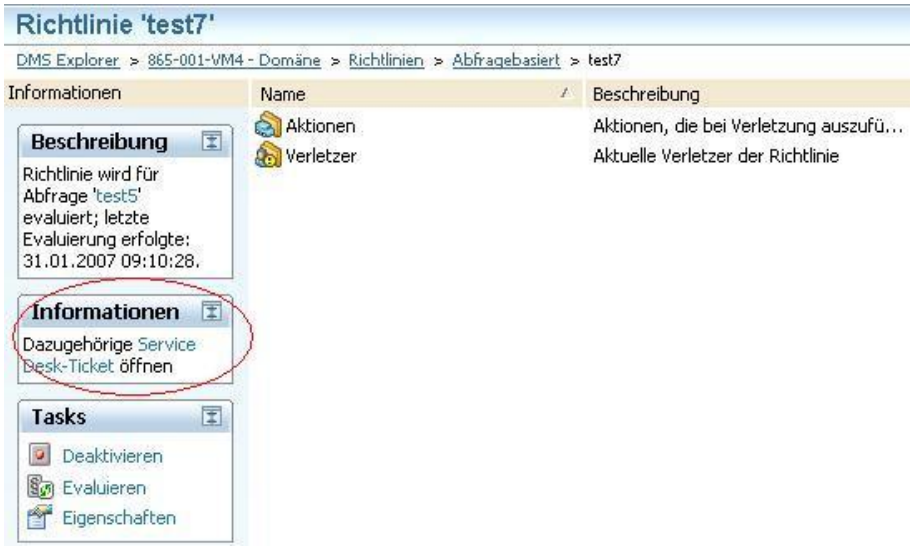
- einem fehlgeschlagenen Softwarejob (siehe Seite 517)
- einer Verletzung einer Asset-Richtlinie (siehe Seite 518)

Ticketdetails im Kontext eines fehlgeschlagenen Softwarejobs

Softwarejobs, die fehlschlugen und ein CA Service Desk Manager-Ticket auslösten, bewirken den Eintrag "Service Desk-Ticket öffnen" im Kontextmenü, das angezeigt wird, wenn Sie mit der rechten Maustaste auf den fehlgeschlagenen Softwarejob klicken. Durch die Auswahl von "Service Desk-Ticket öffnen" wird die CA Service Desk Manager-Web-GUI gestartet.

Ticketdetails im Kontext einer Verletzung der Asset-Richtlinie

Wenn eine Richtlinie CA Service Desk Manager-aktiviert ist, wird in der Spalte "Informationen" im DSM-Explorer der zusätzliche Hyperlink "Zugehöriges Service Desk-Ticket öffnen" angezeigt. Wenn Sie diesen Hyperlink auswählen, wird die CA Service Desk Manager-Ticket-Detailanzeige gestartet, die ursprünglich durch eine Verletzung dieser Richtlinie erzeugt wurde.



Erstellen eines Tickets im Kontext eines verwalteten Assets (Ad-hoc)

CA Service Desk Manager-Tickets werden interaktiv erstellt, indem Sie im Portlet "Schnellstart" auf die Aktion "Service Desk-Ticket erstellen" klicken.

Das Portlet "Schnellstart" befindet sich auf der Registerkarte "Startseite", die geöffnet wird, wenn Sie im DSM-Explorer ein verwaltetes Asset auswählen.

Die Methode zum Erstellen von Tickets ist auch als Befehl im Kontextmenü "Assets" verfügbar.

Kontextabhängiger Start von CA Service Desk Manager zu CA ITCM

Der DSM-Explorer und die Webkonsole werden über einzelne URLs in der CA Service Desk Manager-Web-GUI gestartet.

Der Hyperlink, der den DSM-Explorer oder die DSM-Webkonsole startet, wird in den Übersichtsinformationen im Feld "Zusammenfassung" des CA Service Desk Manager-Tickets angezeigt.

Hinweis: Wenn der DSM-Explorer mit dem Befehl "dsmgui.exe" gestartet wird, muss der Explorer auf dem CA Service Desk Manager-Computer neu installiert werden, der die CA Service Desk Manager-Web-GUI ausführt.

Einrichten von CA Service Desk Manager und CA ITCM

Der CA Service Desk Manager-Setup installiert automatisch die Service-Aware-Richtlinie für CA ITCM und die vordefinierten Problemtypen zum Erstellen von Tickets. Der Name der Service-Aware-Richtlinie ist "ManagedAssetEvents". Die vordefinierten Problemtypen können jederzeit vom CA Service Desk Manager-Administrator geändert oder erweitert werden.

Darüber hinaus erstellt CA Service Desk Manager ein Proxy-Konto für CA ITCM, System_MA_User, das mit einem festgelegten Satz von Berechtigungen konfiguriert ist, und stellt mit der Service-Aware-Richtlinie eine Verknüpfung her.

Der CA ITCM-Setup erstellt automatisch eine Konfigurationsrichtlinine zur Integration in CA Service Desk Manager. Die Konfigurationsrichtlinie wird auf dem allgemeinen Konfigurations-Manager (CCNF) unter folgendem Pfadnamen installiert:

```
/Default Computer Policy/DSM/Service Desk Integration/default
```

Um die Integration zu aktivieren, muss der CA ITCM-Administrator die Konfigurationsrichtlinie über die Benutzeroberfläche des Allgemeinen Konfigurations-Managers einrichten

Zu den Parametern der Konfigurationsrichtlinie gehören folgende Bereiche:

- Ein Schalter, der angibt, ob die CA Service Desk Manager-Integration aktiviert ist.
- Sichere Anmeldungsparameter beim CA Service Desk Manager-Webdienst
- Die URL zum CA Service Desk Manager-Webdienst

Voraussetzung für einen Start von CA Service Desk Manager innerhalb des Kontextes

Die Integration von CA Service Desk Manager unterstützt kontextabhängige Starts des DSM-Explorers in der CA Service Desk Manager-Web-GUI. Diese Starts setzen voraus, dass Sie über geeignete Zugriffsberechtigungen verfügen, die in CA Service Desk Manager gewährt wurden. Daher muss das Benutzerkonto (Benutzer-ID und Kennwort), mit dem Sie sich beim DSM-Explorer angemeldet haben, als Kontakt in CA Service Desk Manager erstellt werden.

Wenn Ihr CA ITCM-Benutzerkonto in CA Service Desk Manager unbekannt ist, wird Ihnen ein Anmeldebildschirm angezeigt, wenn Sie versuchen, die CA Service Desk Manager-Web-GUI zu starten.

Voraussetzungen für die CA Service Desk Manager-Integration in mehreren Engines

Wenn Sie zum Bewerten von Richtlinien mehrere Engines verwenden, muss die CA Service Desk Manager-Integration für alle Systeme aktiviert werden, in denen eine Engine ausgeführt wird, d. h., dass auf allen Systemen die folgenden Voraussetzungen erfüllt sein müssen:

- Ein Agent ist installiert und wird ausgeführt.
- Die Konfigurationsrichtlinie, die die CA Service Desk Manager-Integration aktiviert, wurde auf diesen Agenten gezogen und abgelegt.
- Die Zertifikatdatei ".p12" wird importiert (wenn die verwaltete Methode verwendet wird).

Voraussetzungen für die CA Service Desk Manager-Integration im Enterprise-Manager

Um die CA Service Desk Manager-Integration auf einem Enterprise-Manager zu aktivieren, müssen auf einem Enterprise-Manager folgende Voraussetzungen erfüllt sein:

- Ein Agent ist installiert, wird ausgeführt und ist mit einem der verknüpften Domänen-Manager verbunden.
- Die Konfigurationsrichtlinie, die die CA Service Desk Manager-Integration aktiviert, wurde auf diesen Agenten gezogen und abgelegt.
- Die Zertifikatdatei ".p12" wird importiert (wenn die verwaltete Methode verwendet wird).

Informationen zur CA ITCM- und CA Service Desk Manager-Integration

Im Folgenden finden Sie wichtige Hinweise zu Ihren CA ITCM- und CA Service Desk Manager-Integrationsszenarien:

- Software Delivery-Job von einem für Service Desk aktivierten Enterprise-Manager (siehe Seite 522)

Software Delivery-Job von einem Enterprise-Manager, der für Service Desk aktiviert ist

Folgendes gilt für die Szenarien, in denen eine CA ITCM- und CA Service Desk Manager-Integration auf einem Enterprise-Manager durchgeführt wird.

Ein Software Delivery-Job, der von einem Enterprise-Manager gestartet wird, der für Service Desk aktiviert ist, erstellt kein Service Desk-Ticket, wenn er aufgrund von auf dem Enterprise-Manager oder dem Domänen-Manager beendeten DTS-Plugins fehlschlägt.

Sichere Anmeldung beim CA Service Desk Manager-Webdienst

Der CA ITCM-Administrator kann zwischen zwei Methoden für eine sichere Anmeldung beim CA Service Desk Manager-Webdienst auswählen:

- Einer einfachen Anmeldemethode, die einen Benutzernamen und ein Kennwort erfordert (nicht verwaltete Methode)
- Einer verwalteten Anmeldemethode auf Basis der öffentlichen/privaten Schlüssel und einer eTrust PKI-Verschlüsselung.

Benutzername/Kennwort und die Authentifizierung über öffentlichen/privaten Schlüssel sind noch nicht verwendbar. Nach der Installation von CA Service Desk Manager und CA ITCM ist ein weiterer Konfigurationsschritt erforderlich.

Die Methode zum sicheren Anmelden wird über den Parameter sdlogonmanaged in der CA ITCM-Konfigurationsrichtlinie (comstore) angegeben. Der Standardwert für diesen Parameter ist "Managed", d. h., dass die Anmeldung über ein Zertifikat und eine Verschlüsselung/Entschlüsselung auf Basis von eTrust PKI erfolgt. Der Wert "Notmanaged" bedeutet, dass sich der Benutzer mit Benutzername und Kennwort anmeldet.

So konfigurieren Sie die sichere Anmeldung:

Um die sichere Anmeldung zu konfigurieren, muss der CA ITCM-Administrator folgende Konfigurationsschritte ausführen:

1. Wählen Sie die Methode zur Authentifizierung aus.
2. Wenn Sie die nicht verwaltete Methode auswählen, führen Sie folgende Aktionen durch:
   - Erstellen Sie ein entsprechendes Betriebssystemkonto für CA Service Desk Manager.
   - Konfigurieren Sie CA ITCM entsprechend über eine Konfigurationsrichtlinie.
3. Wenn Sie die verwaltete Methode auswählen, führen Sie folgende Aktionen durch:
   - Erstellen Sie ein X.509-Zertifikat mit einem privaten Schlüssel, und legen Sie es mit einer PKCS#12-Datei offen. Administratoren können zu diesem Zweck das Hilfsprogramm CA Service Desk Manager verwenden oder ihre eigenen Zertifikate zur Verfügung stellen.
   - Importieren Sie die erstellte Richtliniendatei mit dem CA ITCM-Hilfsprogramm "cacertutil" in CA ITCM.

Benutzername- und Kennwortmethode (nicht verwaltet)

Die Parameter "sdusr" und "sdpwd" in der Konfigurationsrichtlinie werden jeweils für den Benutzernamen und das Kennwort verwendet.

CA Service Desk Manager-Setup lädt automatisch den Kontakt-System_MA_User zur Verwendung durch CA ITCM und verknüpft ihn mit der CA ITCM-Service-Aware-Richtlinie "ManagedAssetEvents".

Der Standardwert von "sdusr" ist somit "System_MA_User".

Um den Benutzernamen und das Kennwort als Anmeldemethode zu aktivieren, muss der CA Service Desk Manager-Administrator folgende Aktionen durchführen:

- Erstellen Sie einen Benutzer des Betriebssystems.
- Bearbeiten Sie den Kontakt von System_MA_User, und fügen Sie den Betriebssystem-Benutzernamen im Anmeldefeld "System" ein.

  (Die Systemanmeldung ist standardmäßig mit dem System_MA_User identisch.)

Der CA ITCM-Administrator muss die CA ITCM-Konfigurationsrichtlinie mit dem entsprechenden Kontaktnamen und Kennwort aktualisieren, die in CA Service Desk Manager erstellt wurden.

Administratoren können einen anderen Kontakt als den System_MA_User erstellen und verwenden. Daher müssen Sie die Konfiguration in CA Service Desk Manager und die CA ITCM-Konfigurationsrichtlinie synchron ändern.

Zertifikat- oder eTrust PKI-Methode (verwaltet)

CA Service Desk Manager-Setup lädt automatisch den Kontakt-System_MA_User zur Verwendung durch CA ITCM und verknüpft ihn mit der CA ITCM-Service-Aware-Richtlinie "ManagedAssetEvents".

Um das Zertifikat (eTrust PKI) als Anmeldemethode zu verwenden, muss der CA Service Desk Manager-Administrator zwei Schritte ausführen:

- Erstellen einer PKCS#12-Datei (siehe Seite 525).
- Importieren der PKCS#12-Datei in die CA ITCM-Konfigurationsdatei (siehe Seite 526).

Erstellen einer PKCS#12-Datei

Der Administrator kann seine eigenen Schlüssel über eine PKCS#12-Datei zur Verfügung stellen. Der Administrator kann zu diesem Zweck z. B. Zertifizierungsstellen von Drittanbietern verwenden.

Um eine PKCS#12-Datei zu erstellen, führen Sie im CA Service Desk Manager-Hilfsprogramm mit dem Befehl "pdm_pki" folgende Schritte aus:

1. Erstellen eines öffentlichen/privaten Schlüsselpaars.
2. Verknüpfen Sie den öffentlichen Schlüssel mit der CA ITCM-Richtlinie in der CA Service Desk Manager-Datenbank.
3. Erstellen Sie ein X.509-Zertifikat mit dem privaten Schlüssel, und legen Sie es mit einer PKCS#12-Datei offen.

Das Hilfsprogramm pdm_pki erstellt eine PKCS#12-Datei mit dem Namen MANAGED_ASSET_EVENTS.p12 in seinem Arbeitsverzeichnis.

Der Befehl "pdm_pki" hat folgendes Format:

`pdm_pki -p MANAGED_ASSET_EVENTS [-l` *`Zertifikatdatei`*`] [-f]`

-p

Definiert den Richtliniencode. In diesem Fall muss der Wert MANAGED_ASSETS_EVENTS verwendet werden.

-l

Lädt ein Zertifikat aus einer Datei, anstatt ein neues Zertifikat zu erstellen.

-f

Erzwingt das Ersetzen eines bereits bestehenden Schlüssels.

Importieren der PKCS#12-Datei in die CA ITCM-Konfigurationsdatei

Zum Importieren der PKCS#12-Datei in die CA ITCM-Konfigurationsdatei ("comstore") verwenden Sie die das CA ITCM-Hilfsprogramm "cacertutil" wie im Folgenden beschrieben.

Der Befehl cacertutil zum Importieren der PKCS#12-Datei in die CA ITCM-Konfigurationsdatei (comstore) hat folgendes Format:

```
cacertutil import -i:certificate_file
    -ip:MANAGED_ASSET_EVENTS -t:MANAGED_ASSET_EVENTS
    -l:global
```

-i

Gibt den Namen der Zertifikatdatei an.

-ip

Gibt die Passphrase an.

-t

Gibt das Identitäts-Tag an.

-l

Gibt den Benutzer an.

Einstellungen in der Konfigurationsrichtlinie

Konfigurationseinstellungen für die CA Service Desk Manager-Integration werden im Parameterabschnitt "sdintegration" der CA ITCM-Konfigurationsdatei (comstore.xml) angegeben. Parameter in der Konfigurationsdatei werden eingerichtet, um zentral über eine allgemeine Konfigurationsrichtlinie (CCNF) verwaltet zu werden.

Die folgenden Parameter werden für die CA Service Desk Manager-Integration verwendet.

SdIsEnabled

Gibt an, ob die CA Service Desk Manager-Integration aktiviert ist. Wenn der Wert von SdIsEnabled "True" ist, ist die CA Service Desk Manager-Integration aktiviert. Wenn dieser Wert "False" ist, ist die Integration nicht aktiviert.

Standard: False

SdEnd

Gibt die URL zum CA Service Desk Manager-Webdienst an.

Standard: http://*myhost*:8080/axis/services/USD_R11_WebService

Ersetzen Sie *Mein Host* durch die entsprechende Serveradresse Ihres CA Service Desk Manager-Webdienstes. Standard ist Port 8080.

SdLogonManaged

Gibt an, wie die Anmeldung beim CA Service Desk Manager-Webdienst gesteuert wird. Wenn der Wert "Managed" ist, wird die Anmeldung über das PKCS#12-Zertifikat gesteuert. Wenn der Wert "Notmanaged" ist, wird die Anmeldung über das Benutzerkonto und Kennwort gesteuert.

Standard: Verwaltet

SdUsr

Definiert das Benutzerkonto für die Anmeldung beim CA Service Desk Manager-Webdienst. Dieser Parameter wird nur verwendet, wenn "SdLogonManaged" auf "Notmanaged" gesetzt ist.

Standard: System_MA_User

SdPwd

Definiert das Kennwort für die Anmeldung beim CA Service Desk Manager-Webdienst. Dieser Parameter wird nur verwendet, wenn "SdLogonManaged" auf "Notmanaged" gesetzt ist.

Hinweis: Abgesehen vom Konto "SdUsr" ist auch das Konto des derzeit angemeldeten Benutzers wichtig. Wenn im Kontext eines verwalteten Assets in der DSM-Explorer-GUI ein Ad-hoc-Ticket erstellt wird, wird dieses Konto in CA Service Desk Manager als Ersteller des Tickets angegeben. Wenn ein Ticket im Kontext von Asset Management oder Software Delivery erstellt wird, ist der Ersteller des Tickets immer der Administrator.

Standard: *Leer*

SdPolicy

Gibt den Namen der CA Service Desk Manager-Service-Aware-Richtlinie an, bei der die Anmeldung erfolgen soll. Dieser Parameter wird nur verwendet, wenn "SdLogonManaged" auf "Notmanaged" gesetzt ist. Es wird ein PKCS#12-Zertifikat verwendet. Die verwaltete Anmeldung enthält bereits eine Richtlinienbeschreibung, die diesen Wert immer außer Kraft setzt. Wenn dieser Parameter nicht angegeben ist, wird die Standard-CA Service Desk Manager-Richtlinie ausgewählt.

Standard: MANAGED_ASSET_EVENTS

SdThrottle

Gibt an, ob die Netzwerk- und CPU-Drosselung aktiviert ist. Wenn der Wert "True" (Wahr) ist, ist die Drosselung aktiviert. Wenn der Wert "False" (Falsch) ist, ist die Drosselung deaktiviert.

Standard: False

SdTimeout

Gibt das Zeitlimit für Aufrufe des CA Service Desk Manager-Webdienstes an. Der Wert kann verändert werden, um ein Zeitlimit beim Senden, Erhalten und Verbinden zu erzwingen. Positive Werte geben Sekunden vor dem Zeitlimit an, z. B. gibt der Wert "20" ein Zeitlimit nach 20 Sekunden an. Negative Werte geben Millisekunden an, z. B. gibt der Wert "-200" ein Zeitlimit nach 200 Millisekunden an.

Standard: 0 (unendlich)

Kapitel 14: Fehlerbehebung

Dieser Abschnitt enthält die folgenden Themen:

Freigabefehler der CIC-Verbindung

Bei der Freigabe durch den CA Content Import Client (CIC) für eine Verbindung zur Oracle-MDB kann manchmal ein Fehler auftreten, bei der die folgende Fehlermeldung im CIC-Protokoll zurückgegeben wird:

```
[CCMain] WARN  [com.ca.sccc.dbm.CCDBManager] - Failed to uninitialize MDB
connection pool for domain 'xxx'
```

DSM-Engine stürzt bei angehaltener Datenbank ab

Symptom:

Beim Anhalten der Datenbank zur Wartung, um beispielsweise eine Sicherung vorzunehmen, stürzen die Engineprozesse manchmal ab.

Lösung:

Stellen Sie sicher, dass Sie alle Engineprozesse angehalten haben, bevor Sie die Datenbank zur Wartung anhalten.

Hinweis: Wenn ein Engineprozess während der Datenbankwartung abstürzt, starten Sie den Engineprozess nach dem Neustart der Datenbank neu.

Voraussetzungen für SXP Packager unter Windows 8

Wenn Sie versucht haben, Pakete mit SXP Packager auf dem Computer zu erstellen, überprüfen Sie, ob .NET Framework 3.5 auf dem Windows 8- oder Windows Server 2012-Computer installiert und aktiviert ist. Gehen Sie dazu folgendermaßen vor:

Windows 8:

Klicken Sie auf "Systemsteuerung", "Programme und Features", "Windows-Features aktivieren oder deaktivieren". Weitere Informationen finden Sie unter "http://msdn.microsoft.com/en-us/library/hh506443.aspx".

Windows Server 2012:

Installieren Sie .NET Framework 3.5 mit dem Assistenten zum Hinzufügen von Rollen und Features. Weitere Informationen finden Sie unter "http://technet.microsoft.com/en-us/library/hh83180.aspx".

Öffnen der exportierten Berichte

Die exportierten Dateien weisen das Unicode-Format auf. Um die Dateien in einer Anwendung anzuzeigen, die Unicode nicht unterstützt, ändern Sie das Verschlüsselung zu ANSI, bevor Sie die Datei öffnen.

Fehler bei der Verbindung des Alarm-Collectors zum angegebenen Manager

Symptom:

Wenn ich während der Installation des Alarm-Collectors den Alarm-Collector-Statusbefehl ausführe, zeigt der Alarm-Collector folgende Meldung an:

Verbindung zum angegebenen Manager nicht möglich.

Lösung:

Wenn Sie den Alarm-Collector auf einem eigenständigen Server installieren, der so konfiguriert ist, entweder eine Verbindung zum Enterprise-Manager oder zum Domänen-Manager herzustellen, wobei die Verbindung zum Manager fehlschlägt. Der Alarm-Collector stellt erstmals eine Verbindung zum Manager her, um den Manager-Typ (Enterprise-Manager oder Domänen-Manager) zu bestimmen. Wenn eine ungültige Rolle angegeben wurde, wird der Manager-Typ verwendet, um die angegebene Rolle zu überprüfen und um zur Standardrolle zu wechseln.

Überprüfen Sie, ob der CAF ausgeführt wird und auf dem eigenständigen Server und dem Manager funktioniert. Alarm-Collector ruft die erforderlichen Informationen ab und funktioniert ordnungsgemäß. Diese Statusmeldung wird angezeigt, wenn der Manager des Alarm-Collectors geändert und der Alarm-Collector neu gestartet wird. Zum Beheben des Problems treffen dieselben Schritte zu.

Fehler bei der Verbindung des Alarm-Collectors mit der Datenbank

Symptom:

Beim Hochladen der Alarme in den Alarm-Collector werden die hochgeladenen Alarme in WAC nicht mit dem Statusbefehl *AlertCollector* angezeigt. Es wird folgende Meldung angezeigt:

Verbindung zur Datenbank konnte nicht hergestellt werden.

Lösung:

Stellen Sie sicher, dass der Alarm-Collector auf einem eigenständigen Server eine Verbindung mit der Datenbank herstellt, indem Sie die Datenbankserverkonnektivität überprüfen oder die zugehörigen 32-Bit-DB-Client-Tools (beispielsweise SQL- oder Oracle-Clients) auf dem Computer installieren.

DSM-Explorer zeigt kein Aufforderungsfenster bei der Verbindung im Besprechungsmodus an

Symptom:

Wenn ich den DSM-Explorer in einem Domänen-Manager öffne und mit der rechten Maustaste auf einen Agent klicke und eine Verbindung im Besprechungsmodus herstelle, zeigt die Anwendung das Aufforderungsfenster nicht an.

Lösung:

Stellen Sie sicher, dass das libatk-1.0.so.0-Paket auf dem Agent installiert ist.

Probleme mit dem Ändern der Boot-Server-Konfiguration von "tftp" in den Zugriffsmodus "Freigabe" in Cluster-Setup

Symptom:

Wenn ich die Boot-Server-Konfiguration von "tftp" in den Zugriffsmodus "Freigabe" im Cluster-Setup ändere, dann erhalte ich folgenden Fehler:

ERROR: trying to create camenu share
ERROR: trying to create sxpsetup share

Lösung:

Sie können den Zugriffsmodus "Freigabe" als Boot-Server-Konfiguration ohne Fehler im CA ITCM-Anwendungscluster festlegen, indem Sie einen Remote-Scalability-Server konfigurieren.

Problem mit Größendetails der ITCM- und CIC-Komponenten auf "Programme hinzufügen/entfernen"

Symptom:

Nachdem ich CA ITCM Version 12.8 installiert oder ein Upgrade durchgeführt habe, wird unter "Systemsteuerung", "Programme hinzufügen/entfernen" die geschätzte Größe von CA ITCM, Content Import Client (CIC), Patch Manager und anderen CA ITCM-Komponenten nicht angezeigt.

Lösung:

Das Abrufen und Anzeigen der Größe unter "Systemsteuerung", "Programme hinzufügen/entfernen" ist eine Eigenschaft von Windows und nicht von InstallShield. Dieses Verhalten ist auf eine Änderung der Funktion zurückzuführen, die Microsoft verwendet, um die geschätzte Größe unter Windows zu berechnen. Die Größe jeder installierten Komponente wird mithilfe des BS-Algorithmus geschätzt. Dieser Algorithmus kann in unterschiedlichen Windows-Versionen variieren, wodurch die Anzeige der geschätzten CA ITCM-Größe beeinflusst wird.

Um die geschätzte Größe aufzufüllen, können Sie folgende Schritte ausführen:

Gehen Sie wie folgt vor:

Microsoft verwendet exklusiv Registrierungsschlüssel "*EstimatedSize*", um den geschätzten Größenwert in "Programme hinzufügen/entfernen" aufzufüllen. Um die geschätzte Größe aufzufüllen, können Sie den Registrierungsschlüssel "*EstimatedSize*" in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{PRODUCT_CODE} manuell bearbeiten. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

Fehler und Verzögerungen beim Zugriff auf den technischem Support

Symptom:

Wenn ich versuche, auf die Seite des technischen Supports über die CA ITCM-Infobildschirme zuzugreifen, wird nach einiger Verzögerung ein Skriptfehler angezeigt.

Lösung:

Klicken Sie auf "Ja", und die Seite des technischen Supports wird nach einer kleinen Verzögerung angezeigt. Hinweis: Diese Verzögerung tritt nur im Internet Explorer 7 auf.

SE-Linux-Support für CA ITCM-Komponenten

Linux-Systeme, auf denen das SE-Linux-Sicherheitssystem aktiviert ist, erfordern bestimmte SE-Linux-Einstellungen für die folgenden CA ITCM-Komponenten:

DSM-Webservices und -Webkonsole

Die CA ITCM-Webservices und -Webkonsole können erfolgreich auf Systemen installiert werden, auf denen für SE-Linux der Modus "enforcing" festgelegt ist. Für die Arbeit mit diesen Komponenten müssen Sie jedoch wie folgt in den Modus **permissive** wechseln:

Gehen Sie wie folgt vor:

- Öffnen Sie die Datei "/etc/selinux/config" in einem Texteditor.
- Ändern Sie das Flag SELINUX=enforcing in SELINUX=**permissive.**
- Starten Sie das System neu.

Unverständlicher Text auf der Benutzeroberfläche des japanischen Installationsprogramms

Gilt für die japanische Linux-Version

Symptom:

Wenn ich die japanische Version des Installationsprogramms unter Linux starte, wird unverständlicher Text auf der Benutzeroberfläche angezeigt.

Lösung:

Starten Sie das Produktinstallationsprogramm im Befehlszeilenmodus oder führen Sie die automatische Installation mit der Antwortdatei aus.

Problem mit Zeichenfolgen an der Eingabeaufforderung

Gültig für Windows und Linux

Symptom:

Wenn ich Befehle in einer lokalisierten Umgebung ausführe, gibt es Probleme mit den Zeichenfolgen an der Eingabeaufforderung.

Lösung:

Um das Problem mit Zeichenfolgen an der Eingabeaufforderung zu beheben, nehmen Sie die folgenden Änderungen vor:

(Unter Windows)

Dieses Problem tritt auf, wenn die Standardcodepage der Umgebung nicht unterstützt wird.

Beispiel: Wenn die Standardcodepage für Deutsch und Französisch 850 ist, werden Zeichenfolgen an der Eingabeaufforderung fehlerhaft angezeigt. Beachten Sie, dass CA ITCM für Deutsch und Französisch die *Codepage 1252* unterstützt.Sie können die Codepage in den Umgebungseinstellungen zurücksetzen, indem Sie den folgenden Befehl ausführen:

```
chcp 1252
```

(Für Linux)

Sie können den Sprachparameter wie folgt zurücksetzen:

1. Navigieren Sie zum Ordner *cd\etc\sysconfig*, und öffnen Sie *i18n.*
2. Ändern Sie den Parameter Lang wie folgt:

   Beispiel:
   (Für Deutsch) Lang=de_DE.UTF-8

   (Für Französisch) Lang=fr_FR.UTF-8

Fehler beim Laden von gemeinsam genutzten Bibliotheken auf einem neueren 64-Bit-Linux-Betriebssystem

Symptom:

Einige der DSM-Funktionen (wie cfSysTray, Remote Control-Verbindung, DSM-Eigenschaften) funktionieren auf einem neueren 64-Bit-Linux-Betriebssystem nicht richtig. Bei der Ausführung von "cfSystray" wird zum Beispiel die folgende Fehlermeldung angezeigt:

[root@hostname]# cfsysTray show
cfSysTray: error while loading shared libraries: libgtk-x11-2.0.so.0: wrong ELF class: ELFCLASS64.

Lösung:

DSM ist eine 32-Bit-Anwendung und erfordert 32-Bit-Versionen der BS-Bibliotheken. DSM-Befehle sind fehlgeschlagen, weil das 64-Bit-Linux-Betriebssystem keine 32-Bit-BS-Bibliotheken umfasst. Diese Bibliotheken werden nicht standardmäßig auf den neueren 64-Bit-Linux-Betriebssystemen installiert.

Um die erforderlichen Bibliotheken zu installieren, setzen Sie sich mit dem CA Support oder Ihrem Systemadministrator in Verbindung.

Agenteninstallation schlägt unter Solaris mit einem Fehler fehl

Symptom:

Die Agenteninstallation ist unter Solaris 10 mit dem folgenden Fehler in der Protokolldatei fehlgeschlagen:

ld.so.1: setup: fatal: libCstd.so.1: version `SUNW_1.4.2' not found (required by file /opt/CA/DSM/capki/setup)
ld.so.1: setup: fatal: libCstd.so.1: open failed: No such file or directory Killed /opt/CA/DSM/capki/setup install caller=CAITCM verbose env=all failed with return code = 137
11:43:58 !! Skript mit Fehler ausgeführt: 137
Das Skript oder der Befehl "capki/pkiInst" ist mit Beendigungscode 137 fehlgeschlagen.
Ursache: Mit dem Skript oder Befehl ist ein Problem aufgetreten.
Aktion: Suchen Sie weitere Details in der Installationsprotokolldatei "/opt/CA/SharedComponents/installer/log/ca-dsm.log".

Lösung:

Die Agenteninstallation unter Solaris 10 ist fehlgeschlagen, weil die Version der libCstd-Bibliothek nicht kompatibel ist. Um dieses Problem zu lösen, installieren Sie den Solaris BS-Patch 119964-12 oder höher.

Remote Control unter Windows 8 Sicherer Modus

Symptom:

Remote Control unter Windows 8 und Windows Server 2012 unterstützt alle Verbindungsmodi außer den sicheren Steuerungsmodus.

Lösung:

Die Lösung ist in Bearbeitung und für unsere nächste größere Version geplant.

Verbindung mit MDB kann nicht hergestellt werden

Symptom:

Während der Installation von CIC wird das Installationsprogramm mit folgender Fehlermeldung angehalten:

Verbindung mit MDB kann nicht hergestellt werden. Überprüfen Sie die MDB-Anmeldeinformationen.

Lösung:

Stellen Sie sicher, dass die MDB-Anmeldeinformationen die Kennwortrichtlinien erfüllen. CIC unterstützt beim MDB-Kennwort alphanumerische Zeichen und folgende Sonderzeichen:

SQL

~ ! # $ * ( ) _ + - { } [ ] ? / @

Oracle

$ _

- Setzen Sie das MDB-Kennwort zurück, und das Installationsprogramm wird erfolgreich ausgeführt.

Weitere Informationen zu den Kennwortrichtlinien der MS SQL- und Oracle-Datenbank finden Sie auf den jeweiligen Websites der Unternehmen.

Der DSM-Manager kann nach dem CAM-Upgrade nicht gestartet werden

Bei der Installation von CA ITCM 12.8 wird CA Message Queuing (CAM) während des Installationsvorgangs für gewöhnlich aktualisiert. Wenn der DSM-Manager nicht gestartet werden kann, da er keine Verbindung zu CAM herstellen kann, halten Sie die aktuell ausgeführte CAM-Version an, oder nehmen Sie nach der CA ITCM-Installation einen Neustart vor.

Protokolle im temporären Ordner werden gelöscht

Symptom:

Bei der Installation von CA ITCM auf dem Computer, auf dem Remotedesktopdienste konfiguriert sind, werden die Protokolle im temporären Ordner gelöscht, nachdem sich der Benutzer abgemeldet hat oder wenn der Computer neu gestartet wird.

Lösung:

Tun Sie Folgendes:

- Navigieren Sie auf dem Computer zu *Remotedesktopdienste, Remotedesktop-Sitzungshost, Temporären Ordner beim Beenden nicht löschen*.
  - Wenn der Status auf "Aktiviert" festgelegt ist, bleiben die temporären Ordner pro Sitzung des Benutzers erhalten, wenn sich der Benutzer aus einer Sitzung abmeldet.
  - Wenn der Status auf "Deaktiviert" festgelegt ist, werden temporäre Ordner gelöscht, wenn sich der Benutzer abmeldet, selbst wenn der Administrator anderweitige Festlegungen im Remotedesktop-Sitzungshostkonfigurations-Tool getroffen hat.
  - Wenn der Status auf "Nicht konfiguriert" festgelegt ist, löschen die Remotedesktopdienste die temporären Ordner vom Remote-Computer bei der Abmeldung, sofern nicht anderweitig vom Serveradministrator festgelegt.

Hinweis: Der Pfad zu Remotedesktopdienste ist von BS-Version zu BS-Version unterschiedlich.

Stabilitätsprobleme des MDB-Installationsprogramms bei falscher Angabe der Variable "ORACLE_HOME" oder "ca_itrm Password"

Wenn die Umgebungsvariable "ORACLE_HOME" falsch festgelegt ist, hängt sich das MDB-Installationsprogramm bei unbeaufsichtigten Installations-, Neuinstallations- oder Aktualisierungsvorgängen auf. Legen Sie die entweder die Variable "ORACLE_HOME" richtig fest, oder entfernen Sie den Wert in dieser Umgebungsvariable. Der Wert für "ORACLE_HOME" wird dann von der Antwortdatei übernommen.

Wenn Sie während der Neuinstallation oder bei einer Aktualisierung ein falsches "ca_itrm"-Kennwort angegeben haben (entweder interaktiv oder unbeaufsichtigt), hängt sich das MDB-Installationsprogramm auf. Überprüfen Sie, ob das richtige "ca_itrm"-Kennwort eingegeben wurde.

Installationsfehler bei der benannte Instanz und der Port-ID

Ein Installationsfehler kann unter Microsoft SQL Server aufgrund der Eigenschaften der benannten Instanz und der Port-ID auftreten. Überprüfen Sie, ob Sie die richtige Port-ID angegeben haben.

Antwortdatei enthält ungenutzte Einträge

Die generierte Antwortdatei und die Vorlage "install.rsp" enthalten die folgenden Microsoft SQL-Einträge: "ITRM_DBSQLPORT=1433" und "ITRM_SQLADMINUSER=sa". Diese Eingaben werden vom MDB-Installationsprogramm nicht genutzt und daher ignoriert.

Fehler bei der Synchronisierung von der SQL-MDB zur Oracle-Ziel-MDB

Symptom:

Bei der Ausführung einer Synchronisierung von einer Quelle mit einer MDB auf SQL Server zu einem Ziel mit einer MDB auf Oracle 11g wird der folgende Fehler in den Engine-Protokollen für ITCM R12.5 SP1 angezeigt:

RecImpl_Ado |RecImpl_Ado.cpp |001371|ERROR | FieldLng encounters an undefined VT type =5 for 14

RecImpl_Ado |RecImpl_Ado.cpp |001373|ERROR | FieldLng encounters an undefined VT type =0

Lösung:

Wenden Sie das Testfix RO43621 an. Folgen Sie den Anweisungen in der "testfix"-Readme.

Fehler bei der Synchronisierung auf eine Ziel-MDB auf Oracle

Symptom:

Bei der Ausführung einer Synchronisierung mit einer Ziel-MDB, die sich auf Oracle befindet, wird die folgende Fehlermeldung in der Engine-Protokolldatei angezeigt:

```
ERROR  | ERROR:OCIStmtExecute() failed
```

Lösung:

Wenden Sie das Testfix RO43619 an. Folgen Sie den Anweisungen in der "testfix"-Readme.

Fehler bei der vereinheitlichten Anmeldung in der Webkonsole auf einem eigenständigen WAC

Symptom:

Beim Zugriff auf die Funktion "Vereinheitlichte Anmeldung" der Webkonsole über einen unterstützten Browser unter Windows 2008 und höher treten bei der Anmeldung Fehler auf, und es wird die Aufforderung angezeigt, sich explizit anzumelden.

Lösung:

Gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass der sich Domänencontroller mit der folgenden lokalen Richtlinieneinstellung mindestens unter Windows 2008 befindet:
   - Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten: Klassisch
   - Netzwerksicherheit: LAN Manager-Authentifizierungsebene: LM- und NTLM-Antworten senden
   - Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Clients) darf keinen Mindestwert aufweisen
2. Stellen Sie sicher, dass der Domänen-Manager unter Windows 2008 und höher ausgeführt wird, und legen Sie die lokale Richtlinie wie in Schritt 1 fest.
3. Stellen Sie sicher, dass die Registrierung des Domänen-Managers unter Windows 2008 und höher ausgeführt wird, und deaktivieren Sie das Kontrollkästchen "Loopback":
   Gehen Sie folgendermaßen vor:
   a. Klicken Sie "Start", "Ausführen".
   b. Geben Sie "regedit" ein. Klicken Sie auf "OK".
   c. Suchen Sie im Registrierungs-Editor nach dem folgenden Registrierungsschlüssel, und klicken Sie darauf: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
   d. Klicken Sie mit der rechten Maustaste auf "LSA", und zeigen Sie auf "Neu". Klicken Sie auf den Wert "DWORD".
   e. Geben Sie "DisableLoopbackCheck" ein. Drücken Sie die EINGABETASTE.
   f. Klicken Sie mit der rechten Maustaste auf "DisableLoopbackCheck". Klicken Sie auf "Ändern".
   g. Geben Sie "1" im Datenfeld "Wert" ein. Klicken Sie auf "OK".
4. Überprüfen Sie die Einstellungen des Browsers (IE oder Firefox) im Feld des Benutzers.

Hinweis: Weitere Informationen über Browsereinstellungen für die vereinheitlichte Anmeldung finden Sie im Thema "Konfigurieren Sie die Browser-Einstellungen für vereinheitlichte Anmeldung" in der *Webkonsolen-Hilfe*.

5. Wenn sich der Browser auf einem Server befindet, befolgen Sie die in Schritt 1 angegebenen lokalen Richtlinieneinstellungen.

Hohe CPU-Auslastung nach DSM-Manager-Upgrade

Symptom:

Nach der Aktualisierung des DSM-Managers auf die aktuelle Version liegt aufgrund alter Kryptografiemodule, die Tomcat 7 oder JRE 1.7 ausführen, eine hohe CPU-Auslastung vor.

Lösung:

Dieses Problem tritt auf, wenn Sie ITCM nur mit dem DSM-Manager aktualisieren und den Patch-Manager nicht aktualisieren. Aktualisieren Sie den Patch-Manager auf die aktuelle ITCM-Version.

Fehler bei der Infrastrukturbereitstellung bei vorhandenem virtuellen Computer unter Windows 2012

Symptom:

Bei der Infrastrukturbereitstellung tritt ein Fehler auf, wenn einer der folgenden Punkt ein virtueller Computer unter Windows 2012 ist.

- Domänen-Manager
- Scalability-Server
- Zielcomputer

Lösung:

Informationen finden Sie im VMware Knowledge Base-Eintrag: "Possible data corruption after a Windows 2012 virtual machine network transfer (2058692)".

Anhang A: Automatisierungsdienst-Konfigurationsdatei

Die Automatisierungsdienst-Konfigurationsdatei enthält Konfigurationsparameter, welche die automatisierte Migration für verschiedene Tasks verwendet. Obwohl alle Parameter in diesem Abschnitt beschrieben werden, sind einige Parameter nur informatorisch. Wir empfehlen, die Parameter, die nur zur Information dienen, nicht zu ändern.

Hinweis: Ein Ganzzahlwert in der automation.config-Datei darf keine Leerzeichen enthalten oder davon umgeben sein. Wenn Sie einen Ganzzahlwert in der automation.config-Datei angeben, überprüfen Sie, dass es keine Leerzeichen in oder um den Wert herum gibt. Leerzeichen im Ganzzahlwert können zu Fehlverhalten des Automatisierungsdienstes führen.

AssessmentServiceEPR

Definiert die Endpunkt-URL des Bewertungsdienstes. Dieser Parameter dient nur zur Informatione.

ITCMEPR

Definiert die Endpunkt-URL des CA ITCM PAM-Webservices. Dieser Parameter dient nur zur Informatione.

ITPAMEPR

Definiert die Endpunkt-URL des CA IT PAM-Webservices. Dieser Parameter dient nur zur Informatione.

AutomationServiceEPR

Definiert die Endpunkt-URL des Automatisierungsdienstes. Dieser Parameter dient nur zur Informatione.

JNI_BIN_PATH

Definiert den JNI-Pfad, um comstore-Werte abzurufen. Dieser Parameter dient nur zur Informatione.

DEFAULT_MANAGER

Definiert den Namen des Standardmanagers für die Webkonsole und CA ITCM-Webservices. Dieser Parameter dient nur zur Informatione.

WipeAndReloadProcess

Definiert den Pfad zur CA IT PAM-Prozessdefinition für Migration durch Bereinigen und Neuladen. Ändern Sie diesen Parameter nur, wenn Sie die Prozessdefinition angepasst haben.

MachineReplacementProcess

Definiert den Pfad zur CA IT PAM-Prozessdefinition für die Rechnerersatzmigration. Ändern Sie diesen Parameter nur, wenn Sie die Prozessdefinition angepasst haben.

MaxNumberOfITPAMInstances

Definiert die Höchstanzahl von CA IT PAM-Instanzen, die ein Automatisierungsdienst gleichzeitig ausführen kann. Je nach Last, die Ihr CA IT PAM-Server verarbeiten kann, ändern Sie diesen Wert.

Hinweis: Der Automatisierungsdienst erstellt eine CA IT PAM-Instanz pro Computer im Migrationsjob.

ProcessLaunchInterval

Definiert das Zeitintervall (in Sekunden) zwischen der Erstellung von CA IT PAM-Instanzen.

TimeOutForOSIMJobs

Definiert das Zeitlimit (in Sekunden), innerhalb dessen der Computer den OSIM-Job starten muss. Nach Überschreiten des Zeitlimits werden die OSIM-Jobs abgebrochen und der BS-Migrationsjob schlägt für den Computer fehl.

WaitForBootServer

Gibt an, dass die Aktivierung der BS-Installation wartet, bis ein Boot-Server das Ziel erfasst und es dem Domänen-Manager meldet.

WaitForOSImage

Gibt an, dass die Aktivierung der BS-Installation wartet, bis das erforderliche BS- und Boot-Image auf dem zugewiesenen Boot-Server verfügbar ist.

WakeOnLAN

Gibt an, ob der Boot-Server den Zielcomputer vor der BS-Installation aktivieren muss.

Reboot

Gibt an, ob der Boot-Server den Neustart auf dem Zielcomputer erzwingen soll, bevor die Installation aktiviert wird, wenn "true" (wahr) festgelegt ist.

ContainerPriority

Definiert die Priorität für Software-Jobcontainer, die für den Migrationsjob erstellt wurden.

DeliveryCalender

Gibt den Namen des zu verwendenden Lieferungskalenders an. Lassen Sie diesen Parameter leer, wenn Sie keinen Lieferungskalender verwenden möchten.

IgnoreJobCalendarsOnTargetComputers

Gibt an, ob die Joboption "Jobkalender auf Zielcomputern ignorieren" festgelegt werden soll, wenn ein RAC-Container erstellt wird. Wird diese Richtlinie auf "Falsch" gesetzt, werden die Kalender nicht auf den Zielcomputern ignoriert. Wenn "True" angegeben ist, werden Kalender auf Zielcomputern ignoriert.

JobsTriggerSS

Gibt an, dass der Scalability-Server den Job zur geplanten Zeit initiieren und ausführen muss.

RemoveInstallationHistory

Gibt an, dass vorhandene Installationsdatensätze gelöscht werden, und verhindert so, dass der Job mit dem Status "Bereits installiert" fehlschlägt, bevor der Installationsprozess aktiviert ist.

RunFromSS

Bestimmt, ob das Jobprüfungsprogramm des Zielcomputers während der Jobausführung die Kommunikation mit dem Server freigeben soll. Nach Abschluss des Jobs stellt der Agent erneut eine Verbindung zu dem Server her und meldet den Jobstatus.

TimesRelativeToEM

Gibt an, dass die angegebene Aktivierungszeit als universelle Zeit interpretiert werden soll. Die auf jedem Domänen-Manager konfigurierte Uhrzeitabweichung wird berücksichtigt, um die empfangene Zeit in die lokale Systemzeit zu konvertieren.

UseDeliveryCalender

Gibt an, ob der Lieferungskalender für den Job verwendet werden soll.

SoftwareBlackList

Definiert die Liste von Softwarepaketen, die verwendet werden, um Computer aus BS-Migrationsjobs auszuschließen. Die Computer, die eines dieser Softwarepakete installiert haben, werden automatisch aus der BS-Migration ausgeschlossen.

MaximumDelayOfJobContainer

Definiert die Zeit, die der Jobcontainer auf zusätzliche Computer wartet, nachdem er den ersten Computer hinzugefügt hat, bevor er den Container versiegelt. Zusätzliche Container werden im Bedarfsfall automatisch erstellt.

MaxNumberOfTargetsPerJobContainer

Definiert die Höchstanzahl von Zielcomputern pro Jobcontainer. Nachdem der Jobcontainer dieses Limit erreicht hat, wird der Container geschlossen und ein neuer Jobcontainer für die verbleibenden Computer erstellt.

LastTargetInContainerOptimization

Gibt an, ob der Jobcontainer sofort aktiviert werden soll, wenn es im Migrationsjob keine weiteren Ziele gibt. Der Container wird sofort aktiviert, auch wenn die Ziele im Container weniger als die in MaxNumberOfTargetsPerJobContainer angegebene Zahl ist, und ohne die Zeit für MaximumDelayOfJobContainer abzuwarten. Dieser Parameter dient nur zur Informatione.

Standard: True

RenamePackageName

Definiert das Umbennungs-Softwarepaket, das zum Umbennen der Computer verwendet wird. Dieser Parameter dient nur zur Informatione.

RenamePackageVersion

Definiert die Version des Umbennungs-Softwarepakets, das zum Umbennen der Computer verwendet wird. Dieser Parameter dient nur zur Informatione.

RenameProcedure

Definiert das Umbennungs-Softwarepaketvorgang, der zum Umbennen der Computer verwendet wird. Dieser Parameter dient nur zur Informatione.

AutomationJobScheduleInterval

Definiert die Zeitverzögerung (in Sekunden), die der Automatisierungsdienst abwartet, bevor der nächste Automatisierungsjob geplant wird.

AutomationJobSchedulerBatchSize

Definiert die Anzahl von Zielen, die vom Automatisierungsdienst geplant werden, bevor der ITPAM-Instanzenstatus für die geplanten Ziele überprüft wird und der Status als "Migration erfolgreich" oder "Migration fehlgeschlagen" angegeben wird. Je nach der Last auf dem CA IT PAM-Server und wie häufig Sie den Status des Ziels aktualisieren möchten, können Sie diesen Wert ändern.

Log4j-Eigenschaften

Definiert die folgenden log4j-Eigenschaften:

– log4j.rootLogger

– log4j.appender.A1

– log4j.appender.A1.layout

– log4j.appender.A1.layout.ConversionPattern

– log4j.appender.A1.MaxFileSize

– log4j.appender.A1.MaxBackupIndex

Zum Beispiel können Sie die folgenden Parameter ändern, um die Protokollebene, die Dateigröße oder die Anzahl von erstellten Protokolldateien zu ändern:

log4j.rootLogger=ERROR, A1

Hinweis: Ändern Sie diesen Wert zu DEBUG oder INFO, um die Protokollebene dementsprechend zu ändern.

log4j.appender.A1.MaxFileSize=5000KB

log4j.appender.A1.MaxBackupIndex=1

Hinweis: Weitere Informationen zu den log4j-Eigenschaften finden Sie in der Dokumentation von org.apache.log4j.PropertyConfigurator.

Anhang B: Von CA IT Client Manager verwendete Ports

Die folgende Tabelle bietet eine detaillierte Beschreibung der Port-Verwendung der verschiedenen DSM-Komponenten. Diese Tabellen sind umfassend und enthalten Duplikate, um für jede Komponente ein vollständiges Bild zur Verfügung zu stellen.

Dieses Kapitel enthält folgende Themen:

Allgemeine Hinweise zur Port-Verwendung (siehe Seite 552)
Vom Enterprise-Manager verwendete Ports (siehe Seite 552)
Vom Domänen-Manager verwendete Ports (siehe Seite 554)
Von Infrastructure Deployment verwendete Ports (siehe Seite 556)
Vom Scalability-Server verwendete Ports (siehe Seite 557)
Vom Boot-Server verwendete Ports (siehe Seite 559)
Von der Engine verwendete Ports (siehe Seite 559)
Vom Agenten verwendete Ports (siehe Seite 561)
Vom Packager verwendete Ports (siehe Seite 562)
Von DSM-Explorer und -Reporter verwendete Ports (siehe Seite 563)
Vom ENC-Gateway verwendete Ports (siehe Seite 564)
Von der Quarantäne des AMT-Assets verwendete Ports (siehe Seite 565)
Verwendung von MDB-Ports (siehe Seite 565)

Allgemeine Hinweise zur Port-Verwendung

Im Allgemeinen müssen für den Großteil der Kommunikation zwischen Komponenten über das Netzwerk nur zwei Ports von CA ITCM geöffnet werden, und zwar UDP-Port 4104 für den (in der Regel geringen) auf Meldungen basierenden Verkehr und TCP-Port 4728 für den (in der Regel umfangreichen) Stream-Verkehr.

Standardmäßig verwendet die Remote-Kommunikation über CA Message Queuing (CAM) UDP über Port 4104, wie in den folgenden Tabellen beschrieben. CAM kann für die Verwendung von TCP für die Remote-Kommunikation konfiguriert werden (was in einigen Fällen vorzuziehen ist). In diesem Fall wird TCP mit einem beliebigen Quell-Port und dem Abhör-Port 4105 verwendet. Die Remote-Kommunikation über CAM mit Hilfe von TCP wird in den Tabellen nicht beschrieben. CAM wird auch in großem Umfang für die lokale Kommunikation verwendet, d. h. die Kommunikation zwischen Komponenten, die auf demselben Computer ausgeführt werden. In diesem Fall wird TCP auf Port 4105 verwendet.

Bestimmte Funktionen innerhalb von CA ITCM können Dateifreigaben verwenden, wenn sie dafür konfiguriert sind. In diesem Fall müssen entsprechende Dateifreigabe-Ports geöffnet werden. Bestimmte Port-Nummern variieren in Abhängigkeit von der Betriebsumgebung (Plattform) und den verfügbaren und konfigurierten Mechanismen.

Typische Dateifreigabe-Ports sind:

Windows

Entweder 139/TCP (alter Stil) oder 445/TCP (neuer Stil)

Linux und UNIX

2049/TCP (NFS)

Vom Enterprise-Manager verwendete Ports

Die folgenden Tabellen bieten eine Übersicht der für die Kommunikation von und zu Enterprise-Manager verwendeten Ports.

Kommunikation vom Enterprise-Manager

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Enterprise-Manager	Alle	Enterprise-Manager	4105	TCP	Alle	Lokale Kommunikation über CAM
Enterprise-Manager	4104	Domänen-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Enterprise-Manager	Alle	Verzeichnisserver	389	TCP	Alle	LDAP-Verzeichniszugriff
Enterprise-Manager	Alle	Verzeichnisserver	636	TCP	Alle	LDAP-Verzeichniszugriff über SSL
Enterprise-Manager	Alle	Domänen-Manager	4728	TCP	Software Delivery	DTS-Dateiübertragung

Kommunikation zum Enterprise-Manager

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Explorer	4104	Enterprise-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Webbrowser	Alle	Enterprise-Manager	80	HTTP	Alle	Webkonsolen-Zugriff
Webdienste-Client	Alle	Enterprise-Manager	80	HTTP	Alle	Zugriff auf Webdienste-API von Remote-Client-Anwendung
Domänen-Manager	Alle	Enterprise-Manager	4728	TCP	Software Delivery	DTS-Dateiübertragung
Explorer	Dateifreigabe-Ports	Enterprise-Manager	Dateifreigabe-Ports	UDP	Software Delivery	NOS-basierte Dateiübertragung
Explorer	Alle	Enterprise-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS
Packager	4104	Enterprise-Manager	4104	UDP	Software Delivery	Kommunikation über CAM im Netzwerk

Hinweise:

- Wenn für die Webkonsole und die Webdienste die Verwendung einer sicheren HTTP-Kommunikation konfiguriert wurde, wird auf dem Domänen-Manager oder dem Enterprise-Manager der Port 443 (Standard) zum Abhören verwendet.
- Die Webkonsole verwendet Apache Tomcat. Standardmäßig ist Tomcat installiert und für die Verwendung der Ports 8080 (Start), 8090 (Beendigung) und 8095 (ajp13) konfiguriert. Diese Ports werden jedoch in der Regel nur lokal verwendet.

Vom Domänen-Manager verwendete Ports

Die folgenden Tabellen bieten eine Übersicht der für die Kommunikation von und zu Domänen-Managern verwendeten Ports.

Kommunikation vom Domänen-Manager

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Domänen-Manager	Alle	Domänen-Manager	4105	TCP	Alle	Lokale Kommunikation über CAM
Domänen-Manager	4104	Enterprise-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Domänen-Manager	4104	Remote-Domänen-Engine	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Domänen-Manager	4104	Scalability-Server	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Domänen-Manager	Alle	Verzeichnisserver	389	TCP	Alle	LDAP-Verzeichniszugriff
Domänen-Manager	Alle	Verzeichnisserver	636	TCP	Alle	LDAP-Verzeichniszugriff über SSL
Domänen-Manager	4104	Explorer	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Domänen-Manager	Alle	Enterprise-Manager	4728	TCP	Software Delivery	DTS-Dateiübertragung: Bestätigungen für Verteilungsauftrag
Domänen-Manager	Alle	Scalability-Server	4728	TCP	Software Delivery	DTS-Dateiübertragung: Paketübertragung

Kommunikation mit Domänen-Manager

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Enterprise-Manager	4104	Domänen-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Explorer	4104	Domänen-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Scalability-Server	4104	Domänen-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Webbrowser	Alle	Domänen-Manager	80	HTTP	Alle	Webkonsolen-Zugriff
Webdienste-Client	Alle	Domänen-Manager	80	HTTP	Alle	Zugriff auf Webdienste-API von Remote-Client-Anwendung
Remote-Domänen-Engine	4104	Domänen-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Agent	4104	Domänen-Manager	4104	UDP	Remote Control Software Delivery	Kommunikation über CAM im Netzwerk SD-Katalog, RC-Host-Auth., RC-Viewer-GAB
Scalability-Server	Alle	Domänen-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS: Jobausgabedateien
Enterprise-Manager	Alle	Domänen-Manager	4728	TCP	Software Delivery	DTS-Dateiübertragung: Paketübertragung
Explorer	Dateifreigabe-Ports	Domänen-Manager	Dateifreigabe-Ports	TCP/UDP	Software Delivery	NOS-basierte Dateiübertragung: Paketregistrierung
Explorer	Alle	Domänen-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS: Paketregistrierung
Packager	4104	Domänen-Manager	4104	UDP	Software Delivery	Steuerungsdaten der Paketregistrierung
Packager	Alle	Domänen-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS: Paketregistrierung

Hinweise:

- Wenn für die Webkonsole und die Webdienste die Verwendung einer sicheren HTTP-Kommunikation konfiguriert wurde, wird auf dem Domänen-Manager oder dem Enterprise-Manager der Port 443 (Standard) zum Abhören verwendet.
- Die Webkonsole verwendet Apache Tomcat. Standardmäßig ist Tomcat installiert und für die Verwendung der Ports 8080 (Start), 8090 (Beendigung) und 8095 (ajp13) konfiguriert. Diese Ports werden jedoch in der Regel nur lokal verwendet.

Von Infrastructure Deployment verwendete Ports

Infrastructure Deployment ist ein Teil des Domänen-Managers. Seine Port-Verwendung wird in einem separaten Abschnitt beschrieben, um hervorzuheben, dass diese Ports nur offen sein müssen, wenn oder während Infrastructure Deployment verwendet wird.

Die in den folgenden Tabellen angegebenen Ports (abgesehen von Port 7) werden verwendet, um den Infrastructure Deployment-Primer vom Domänen-Manager zu entfernen. Wenn ein Kunde bereit ist, den Primer manuell zu installieren oder Infrastructure Deployment überhaupt nicht verwenden möchte, müssen die Ports nicht geöffnet werden. Es ist nicht erforderlich, alle Ports für alle Ziele zu öffnen. Die Ports müssen nicht geöffnet bleiben, sondern müssen nur während der Bereitstellung geöffnet sein.

Darüber hinaus kann der Kunde abhängig von den verwendeten Kommunikationsverfahren eine Teilmenge von MS Share/Telnet- und FTP/SSH-Ports öffnen.

Kommunikation vom Domänen-Manager

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Domänen-Manager	Alle	Ziel	7	TCP	Alle	Echo-Anforderung. Wird während Ziel-Scan verwendet. Die Verwendung dieses Ports kann durch eine entsprechende Einstellung in der Konfigurationsrichtlinie deaktiviert werden.
Domänen-Manager	Dateifreigabe-Ports	Ziel	Dateifreigabe-Ports	TCP UDP	Alle	Windows NOS-basierte Dateiübertragung des Primer-Paketes. Verwendung von ADMIN$
Domänen-Manager	Alle	Ziel	135	TCP	Alle	Windows-RPC-Aufruf zum Start der Primer-Installation
Domänen-Manager	Alle	Ziel	21	TCP	Alle	FTP-basierte Dateiübertragung des Primer-Paketes

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Domänen-Manager	Alle	Ziel	22	TCP	Alle	UNIX ssh/Secure FTP-basierte Dateiübertragung des Primer-Paketes. Vom Domänen-Manager gepusht.
Domänen-Manager	Alle	Ziel	23	TCP	Alle	UNIX Telnet-Verbindung zum Start FTP-basierter Dateiübertragung des Primer-Paketes auf dem Ziel.

Kommunikation mit Domänen-Manager

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Ziel	Alle	Domänen-Manager	20 21	TCP	Alle	FTP-basierte Dateiübertragung des Primer-Paketes

Vom Scalability-Server verwendete Ports

Die folgenden Tabellen bieten eine Übersicht der für die Kommunikation von und zu Scalability-Servern verwendeten Ports.

Kommunikation vom Scalability-Server

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Scalability-Server	Alle	Scalability-Server	4105	TCP	Alle	Lokale Kommunikation über CAM
Scalability-Server	4104	Domänen-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Scalability-Server	4104	Domänen-Engine	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Scalability-Server	4104	Agent	4104	UDP	Alle	Kommunikation über CAM im Netzwerk Konfiguration, SD-Triggerjob-Prüfung, AM-Triggerjob-Prüfung

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Scalability-Server	Alle	Domänen-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS: Jobausgabedateien
Scalability-Server	Alle	Agent	4728	TCP	Software Delivery	DTS-Dateiübertragung: Paketübertragung
Scalability-Server	554	Agent	554	TCP	Software Delivery	RTSP (nicht gesichert) für App-V-Anwendungsdienste
Scalability-Server	322	Agent	322	TCP	Software Delivery	RTSP (gesichert) für App-V-Anwendungsdienste

Kommunikation mit Scalability-Server

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Domänen-Manager	4104	Scalability-Server	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Domänen-Engine	4104	Scalability-Server	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Agent	4104	Scalability-Server	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Agent	Alle	Scalability-Server	4728	TCP	Alle	Dateiübertragung ohne NOS Übertragung von Sicherungsdaten
Agent	Dateifreigabe-Ports	Scalability-Server	Dateifreigabe-Ports	TCP	Software Delivery	NOS-basierte Dateiübertragung
Domänen-Manager	Alle	Scalability-Server	4728	TCP	Software Delivery	DTS-Dateiübertragung: Paketübertragung
Agent	554	Scalability-Server	554	TCP	Software Delivery	RTSP (nicht gesichert) für App-V-Anwendungsdienste
Agent	322	Scalability-Server	322	TCP	Software Delivery	RTSP (gesichert) für App-V-Anwendungsdienste

Vom Boot-Server verwendete Ports

Der Boot-Server ist ein Teil des Scalability-Servers. Seine Port-Verwendung wird in einem separaten Abschnitt beschrieben, um hervorzuheben, dass diese Ports nur offen sein müssen, wenn die Funktionen der BS-Installationsverwaltung verwendet werden.

Kommunikation mit Scalability-Server

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Ziel	68	Scalability-Server	67	UDP	Software Delivery	Bootstrap-Protokoll-Client – bootpc
Ziel	Alle	Scalability-Server	69	UDP	Software Delivery	Trivial File Transfer (TFTP)
PXE-Ziel	Alle	Scalability-Server	4011	UDP	Software Delivery	(Optional) Alternate Service Boot – altserviceboot.binl (PXE) Wenn Port 4011 nicht verfügbar ist, wird stattdessen Port 67 verwendet.
Ziel	Dateifreigabe-Ports	Scalability-Server	Dateifreigabe-Ports	TCP/UDP	Software Delivery	NOS-basierte Dateiübertragung

Von der Engine verwendete Ports

Die folgenden Tabellen bieten eine Übersicht der für die Kommunikation von und zu einer Engine verwendeten Ports.

Kommunikation von der Engine

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Beliebige Engine	Alle	Beliebige Engine	4105	TCP	Alle	Lokale Kommunikation über CAM
Beliebige Engine	Alle	Content-Server	443 oder 5250	TCP	Alle	Softwaresignatur-Download von CA Content-Website

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Beliebige Engine	Alle	Verzeichnisserver	389	TCP	Alle	LDAP-Verzeichniszugriff: Verzeichnissynchronisierung, Abfragen, Berichte
Beliebige Engine	Alle	Verzeichnisserver	636	TCP	Alle	LDAP-Verzeichniszugriff über SSL: Verzeichnissynchronisierung, Abfragen, Berichte
Beliebige Engine	Alle	SMTP-Server	25	TCP/UDP	Asset Management	E-Mail-Versand bei Richtlinienverletzung
Domänen-Engine	4104	Scalability-Server	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Remote-Domänen-Engine	4104	Domänen-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Remote-Enterprise-Engine	4104	Enterprise-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk

Kommunikation zur Engine

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Enterprise-Manager	4104	Remote-Enterprise-Engine	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Domänen-Manager	4104	Remote-Domänen-Engine	4104	UDP	Alle	Kommunikation über CAM im Netzwerk Benachrichtigungen, beispielsweise Ad-hoc-Abfrageevaluierung
Explorer	4104	Beliebige Engine	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Scalability-Server	4104	Domänen-Engine	4104	UDP	Alle	Kommunikation über CAM im Netzwerk

Vom Agenten verwendete Ports

Die folgenden Tabellen bieten eine Übersicht der für die Kommunikation von und zu Agenten verwendeten Ports.

Kommunikation vom Agenten

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Agent	Alle	Agent	4105	TCP	Alle	Lokale Kommunikation über CAM
Agent	4104	Scalability-Server	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Agent	Alle	Scalability-Server	4728	TCP	Alle	Dateiübertragung ohne NOS Übertragung von Sicherungsdaten
Agent	4104	Domänen-Manager	4104	UDP	Remote Control Software Delivery	Kommunikation über CAM im Netzwerk SD-Katalog, RC-Host-Auth., RC-Viewer-GAB
Agent	Dateifreigabe-Ports	Scalability-Server	Dateifreigabe-Ports	TCP	Software Delivery	NOS-Dateiübertragung
Agent	554	Scalability-Server	554	TCP	Software Delivery	RTSP (nicht gesichert) für Microsoft App-V-Streaming-Kommunikation
Agent	322	Scalability-Server	322	TCP	Software Delivery	RTSP (gesichert) für Microsoft App-V-Streaming-Kommunikation

Kommunikation mit dem Agenten

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Explorer	4104	Agent	4104	UDP	Alle	Sofortdiagnose (DSM-Komponenteninfo) SD-Triggerjob-Prüfung AM-Triggerjob-Prüfung

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Scalability-Server	4104	Agent	4104	UDP	Alle	Kommunikation über CAM im Netzwerk Konfiguration SD-Triggerjob-Prüfung AM-Triggerjob-Prüfung
Scalability-Server	Alle	Agent	4728	TCP	Software Delivery	DTS-Dateiübertragung: Paketübertragung
Packager	Alle	Agent	3001, 3002	UDP	Alle	DSM-Dienst-Locator
Explorer	Alle	Agent	4728 *)	TCP	Remote Control	RC-Viewer an RC-Host
Scalability-Server	554	Agent	554	TCP	Software Delivery	RTSP (nicht gesichert) für Microsoft App-V-Streaming-Kommunikation
Scalability-Server	322	Agent	322	TCP	Software Delivery	RTSP (gesichert) für Microsoft App-V-Streaming-Kommunikation

Hinweise:

- *) gibt Folgendes an: Wenn die Legacy-Remote Control-Viewer-Unterstützung aktiviert ist, hört der Remote Control-Host auch TCP-Port 798 ab.
- Ein Scalability-Server kann auf demselben Computer wie ein Domänen-Manager ausgeführt werden.

Vom Packager verwendete Ports

Die folgenden Tabellen bieten eine Übersicht der für die Kommunikation vom Software Management Packager verwendeten Ports.

Kommunikation vom Packager

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Packager	4104	Enterprise-Manager	4104	UDP	Software Delivery	Steuerungsdaten der Paketregistrierung
Packager	Alle	Enterprise-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS: Paketregistrierung

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Packager	4104	Domänen-Manager	4104	UDP	Software Delivery	Steuerungsdaten der Paketregistrierung
Packager	Alle	Domänen-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS: Paketregistrierung
Packager	Alle	Agent	3001, 3002	UDP	Alle	CA ITCM-Dienst-Locator

Von DSM-Explorer und -Reporter verwendete Ports

Die folgenden Tabellen bieten eine Übersicht der für die Kommunikation vom DSM-Explorer sowie vom DSM-Reporter und zum DSM-Explorer verwendeten Ports.

Kommunikation vom Explorer und Reporter

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Explorer	Alle	Explorer	4105	TCP	Alle	Lokale Kommunikation über CAM, Benachrichtigungen
Explorer	4104	Enterprise-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Explorer	4104	Domänen-Manager	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Explorer	4104	Agent	4104	UDP	Alle	Sofortdiagnose (DSM-Komponenteninfo) SD-Triggerjob-Prüfung AM-Triggerjob-Prüfung
Explorer	4104	Beliebige Engine	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Explorer	Alle	Agent	4728	TCP	Remote Control	RC-Viewer an RC-Host
Explorer	Dateifreigabe-Ports	Enterprise-Manager	Dateifreigabe-Ports	UDP	Software Delivery	NOS-basierte Dateiübertragung: Paketregistrierung
Explorer	Alle	Enterprise-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS: Paketregistrierung

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Explorer	Dateifreigabe-Ports	Domänen-Manager	Dateifreigabe-Ports	TCP UDP	Software Delivery	NOS-basierte Dateiübertragung: Paketregistrierung
Explorer	Alle	Domänen-Manager	4728	TCP	Software Delivery	Dateiübertragung ohne NOS: Paketregistrierung

Kommunikation mit Explorer

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
Domänen-Manager	4104	Explorer	4104	UDP	Alle	Kommunikation über CAM im Netzwerk
Enterprise-Manager	4104	Explorer	4104	UDP	Alle	Kommunikation über CAM im Netzwerk

Vom ENC-Gateway verwendete Ports

Die folgende Tabelle bietet eine Übersicht der von der ENC-Gateway-Funktionalität für die Kommunikation verwendeten Ports.

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
ENC-Client	Alle	ENC-Gateway-Server	443	TCP	Alle	ENC-Client-Registrierung, Verbindungsanforderungen, Abhöranforderungen.
ENC-Client	Alle	ENC-Gateway-Server	80	TCP	Alle	Kommunikation über CAM im Netzwerk
ENC-Gateway-Server	Alle	ENC-Gateway-Server	443	TCP	Alle	ENC-Gateway-Server-Registrierung, Weiterleitung von Client-Anforderungen an den ENC-Gateway-Manager, Weiterleitung von Daten zwischen verbundenen ENC-Clients
ENC-Client	Alle	Internet-Proxy	1080	TCP	Alle	Kommunikation über Proxy

Von:	Port	An	Port	Protokoll	Produkt	Beschreibung
ENC-Client	Alle	Internet-Proxy	80	TCP	Alle	Kommunikation über Proxy

Von der Quarantäne des AMT-Assets verwendete Ports

CA IT Client Manager (CA ITCM) unterstützt die Intel Advanced Management Technology (AMT). In diesem Kontext wird eine AMT-Quarantänerichtlinie vorgestellt, bei der es sich um eine Sicherungsfunktion handelt, die AMT-Geräten einen Filter für eingehenden und ausgehenden Netzwerkverkehr hinzufügt.

Die Quarantänerichtlinie liefert einen neuen Managementstatus für ein AMT-aktiviertes Asset. Der Zugriff auf dieses Asset kann vorübergehend gesperrt werden, während das erweiterte Management unter CA ITCM ausgeführt wird. Die Quarantänerichtlinie schließt jeden normalen eingehenden und ausgehenden Datenverkehr mit Ausnahme der Ports, die von AMT-Gerät und von CA ITCM für die Kommunikation verwendet werden, d. h., das in Quarantäne befindliche Intel AMT-Asset kann vollständig von CA ITCM verwaltet werden.

Die Quarantänerichtlinie wirkt sich wie folgt auf Ports aus:

- AMT Senden/Empfangen von ARP-Datenverkehr vom AMT-Computer (Port 67)
- AMT Senden/Empfangen von Datenverkehr auf AMT-Ports (Ports 16992-16995)
- CA ITCM Senden/Empfangen auf Port 4104

  CA ITCM Senden/Empfangen auf Port 4105

  CA ITCM Senden/Empfangen auf Port 4728
- Unterstützung von Port für DHCP-Dienst, wobei Port 53 für Empfangen geöffnet ist.
- Unterstützung von Port für DNS-Dienst, wobei Port 63 für Senden/Empfangen geöffnet ist.

Verwendung von MDB-Ports

Die folgenden Ports werden standardmäßig für die MDB-Kommunikation verwendet:

- Oracle: 1521
- Microsoft SQL Server: 1433

Ein Datenbankadministrator kann die Portzuweisungen am Datenbank-Standort ändern.

Anhang C: Software Delivery-Prozeduren zur Installation

Der Installer in CA IT Client Manager bietet vordefinierte Software Delivery (SD)-Prozeduren für die Installationspakete.

Dieses Kapitel enthält folgende Themen:

Wichtige Hinweise zur Deinstallationsprozedur (siehe Seite 568)
CA DSM Agent + AM, RC, SD Plug-in(s) Linux (Intel) DEU (siehe Seite 568)
CA DSM Agent + Asset Management Plug-In Linux (Intel) DEU (siehe Seite 568)
CA DSM Agent + Basic Inventory Plug-In Linux (Intel) DEU (siehe Seite 569)
CA DMPrimer Linux (Intel) DEU (siehe Seite 569)
SMPackager (Linux) (siehe Seite 569)
CA DSM Remove Legacy Agent Linux (Intel) DEU (siehe Seite 569)
CA DSM Agent + Remote Control Plug-In Linux (Intel) DEU (siehe Seite 569)
CA DSM Agent + Software Delivery Plug-In Linux (Intel) DEU (siehe Seite 570)
CA DSM Scalability-Server Linux (Intel) DEU (siehe Seite 571)
CA DSM Agent + AM, RC, SD Plug-in(s) Win32 (siehe Seite 571)
CA DSM Agent + Asset Management Plug-in (siehe Seite 572)
CA DSM Agent + Basic Inventory Plug-in (siehe Seite 572)
CA DSM Agent + Data Transport Plug-in (siehe Seite 572)
CA DSM Agent + Remote Control Plug-in (siehe Seite 573)
CA DSM Agent + Software Delivery Plug-in (siehe Seite 574)
CA DSM Constant Access (Intel AMT) (siehe Seite 574)
CA DSM eTrust PKI (siehe Seite 575)
CA DSM-Explorer (siehe Seite 575)
CA DSM Manager (siehe Seite 575)
CA DSM-Scalability-Server (siehe Seite 576)
CA DSM Secure Socket Adapter (siehe Seite 576)
CA DSM Remove Legacy Agent Win32 (siehe Seite 577)

Wichtige Hinweise zur Deinstallationsprozedur

Beachten Sie Folgendes, bevor Sie die Deinstallationsprozedur für den Software Delivery (SD)-Agenten verwenden:

- Das SD-Agenten-Plug-In für die Deinstallationsprozedur muss im Jobcontainer an letzter Stelle stehen, da es sich hierbei um das SD-Agenten-Plug-in handelt, das die Paket-Deinstallationsjobs durchführt.
- Da das Data Transport Service (DTS)-Agenten-Plug-In ein separates Paket unter Windows ist, führt die Deinstallation des SD-Agenten nicht implizit zur Deinstallation des DTS-Agenten. Der DTS-Agent muss durch einen separaten Job deinstalliert werden, der jedoch in denselben Jobcontainer aufgenommen werden kann.

CA DSM Agent + AM, RC, SD Plug-in(s) Linux (Intel) DEU

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Installieren
- SM Installer-Installationen scannen
- SWD scannen (scannt die proprietäre Agentendatenbank von SD auf installierte Pakete)
- SWD scannen: Linux-Software
- SM Installer: Tracing deaktivieren
- SM Installer: Tracing aktivieren
- SM Installer: Alle Traces abrufen
- SM Installer: Letztes Trace abrufen
- Alle Komponenten von CA ITCM deinstallieren
- Nur alle Agenten-Plug-ins deinstallieren

CA DSM Agent + Asset Management Plug-In Linux (Intel) DEU

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Installieren
- Alle Komponenten von CA ITCM deinstallieren
- Nur Asset Management-Plug-In deinstallieren

CA DSM Agent + Basic Inventory Plug-In Linux (Intel) DEU

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Installieren
- Alle Komponenten von CA ITCM deinstallieren

CA DMPrimer Linux (Intel) DEU

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Installieren
- Alle Komponenten von CA ITCM deinstallieren

SMPackager (Linux)

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Paket installieren
- Paket erneut installieren
- Paket deinstallieren

CA DSM Remove Legacy Agent Linux (Intel) DEU

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Alle entfernen
- AM entfernen
- SD entfernen

CA DSM Agent + Remote Control Plug-In Linux (Intel) DEU

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Nur zentral verwalteter Host
- Eigenständiger Agent
- Alle Komponenten von CA ITCM deinstallieren
- Nur Remote Control-Plug-In deinstallieren

CA DSM Agent + Software Delivery Plug-In Linux (Intel) DEU

Dieses Installationspaket enthält das Data Transport Plug-In.

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Installieren
- SM Installer-Installationen scannen
- SWD scannen
- SWD scannen: Linux-Software
- SM Installer: Tracing deaktivieren
- SM Installer: Tracing aktivieren
- SM Installer: Alle Traces abrufen
- SM Installer: Letztes Trace abrufen
- Alle Komponenten von CA ITCM deinstallieren
- Nur Software Delivery-Plug-In deinstallieren

CA DSM Scalability-Server Linux (Intel) DEU

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Boot-Server-Freigabe deaktivieren
- MSILIB-Freigabe deaktivieren
- NFS-Freigabe deaktivieren
- Samba-Freigabe deaktivieren
- SDLIB-Freigabe deaktivieren
- Boot-Server-Freigabe aktivieren
- MSILIB-Freigabe aktivieren
- NFS-Freigabe aktivieren
- Samba-Freigabe aktivieren
- SDLIB-Freigabe aktivieren
- Installieren
- CCS-Kalender synchronisieren
- Softwarejob-Datensätze synchronisieren
- Software-Staging-Bibliothek synchronisieren
- Alle Komponenten von CA ITCM deinstallieren
- Nur Scalability-Server + Agenten deinstallieren

CA DSM Agent + AM, RC, SD Plug-in(s) Win32

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Installieren
- Deinstallieren

CA DSM Agent + Asset Management Plug-in

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Erkennen
- Installieren
- Lokale Reparatur
- Deinstallieren
- Verify

CA DSM Agent + Basic Inventory Plug-in

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Erkennen
- Installieren
- Lokale Reparatur
- Deinstallieren
- Verify

CA DSM Agent + Data Transport Plug-in

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Erkennen
- Installieren
- Lokale Reparatur
- Deinstallieren
- Verify

CA DSM Agent + Remote Control Plug-in

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Zentral verwalteter vollständiger Agent
- Nur zentral verwalteter Host
- Erkennen
- Lokale Reparatur
- Eigenständiger Agent
- Deinstallieren
- Verify

CA DSM Agent + Software Delivery Plug-in

Dieses Installationspaket enthält das Data Transport Plug-in nicht.

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Katalog: Hinzufügen
- Katalog: Entfernen
- Erkennen
- Diagnose: Konfigurations- und Versionsinformationen abrufen (dsmdiag-Informationen)
- Installieren
- Lokale Reparatur
- MSI scannen (scannt lokale MSI-Datenbank auf installierte Pakete)
- SM Installer-Installationen scannen (scannt auf dem Agenten installierte SXP-Pakete)
- SWD scannen (scannt die proprietäre Agentendatenbank von SD auf installierte Pakete)
- SM Installer: Tracing deaktivieren
- SM Installer: Tracing aktivieren
- SM Installer: Alle Traces abrufen
- SM Installer: Verlauf abrufen
- SM Installer: Letztes Trace abrufen
- SM Installer: Benutzerverlauf abrufen
- SM Installer: Benutzer-Trace abrufen
- Deinstallieren
- Verify

CA DSM Constant Access (Intel AMT)

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Installieren
- Deinstallieren

CA DSM eTrust PKI

Für dieses Installationspaket ist die folgende Software Delivery-Prozedur vordefiniert:

- Installieren

CA DSM-Explorer

Für dieses Installationspaket sind die folgenden mit Software Delivery (SD) verbundenen Prozeduren vordefiniert:

- Erkennen
- Installieren
- Installieren (ohne Reporter)
- Installieren von AM
- AM installieren (ohne Reporter)
- AM + RC installieren
- AM + RC installieren (ohne Reporter)
- AM + SD installieren
- AM + SD installieren (ohne Reporter)
- Installieren von RC
- RC installieren (ohne Reporter)
- Installieren von SD
- SD installieren (ohne Reporter)
- SD + RC installieren
- SD + RC installieren (ohne Reporter)
- Lokale Reparatur
- Deinstallieren
- Verify

CA DSM Manager

Für dieses Installationspaket ist die folgende Software Delivery-Prozedur vordefiniert:

- Erkennen

CA DSM-Scalability-Server

Das Scalability-Server-Installationspaket hängt vom Paket "CA DSM Agent + Data Transport Plug-in" ab.

Für das Scalability-Server-Paket sind folgende Software Delivery-Prozeduren vordefiniert:

- Erkennen
- Boot-Server-Freigabe deaktivieren
- MSILIB-Freigabe deaktivieren
- SDLIB-Freigabe deaktivieren
- Boot-Server-Freigabe aktivieren
- MSILIB-Freigabe aktivieren
- SDLIB-Freigabe aktivieren
- Installieren
- Lokale Reparatur
- CCS-Kalender synchronisieren
- Softwarejob-Datensätze synchronisieren
- Software-Staging-Bibliothek synchronisieren
- Deinstallieren
- Verify

CA DSM Secure Socket Adapter

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- Installieren
- Deinstallieren

CA DSM Remove Legacy Agent Win32

Für dieses Installationspaket sind folgende Software Delivery-Prozeduren vordefiniert:

- AM entfernen
- RC entfernen
- SD entfernen
- Alle entfernen

Anhang D: Aktuelle Zertifikate von CA IT Client Manager

CA IT Client Manager bietet allgemeine und anwendungsspezifische Zertifikate, die im Folgenden aufgeführt sind. Informationen zum Arbeiten mit und Anpassen von Zertifikaten finden Sie unter "Importieren eigener X.509-Zertifikate in das Installations-Image" (siehe Seite 229) und "Installieren anwendungsspezifischer Zertifikate" (siehe Seite 412).

Dieses Kapitel enthält folgende Themen:

Allgemeine Zertifikate (siehe Seite 579)
Anwendungsspezifische Zertifikate (siehe Seite 580)

Allgemeine Zertifikate

Die allgemeinen DSM-Zertifikate werden im Folgenden aufgeführt.

Standard-DSM-Root-Zertfikat

DN:

CN=DSM Root,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM Root,O=Computer Associates,C=US

Standard-Basis-Hostidentitätszertifikat

DN:

CN=Generic Host Identity,O=Computer Associates,C=US

URI:

x509cert://DSM r11/CN=Generic Host Identity,O=Computer Associates,C=US

Tag:

dsmcommon

Verwendung:

Bereitstellung der Basis-Hostidentität.

Speicherort:

Alle Knoten im Enterprise.

Anwendungsspezifische Zertifikate

Die anwendungsspezifischen Zertifikate werden zur Autorisierung der Sicherheit auf Objektebene in der Management-Datenbank (MDB) verwendet. Wenn Sie neue Zertifikate erstellen, die nicht die Standardnamen verwenden, müssen Sie die Datei "cfcert.ini" mit den neuen URIs vor der Manager-Installation aktualisieren oder neue Sicherheitsprofile mit den Rechten und Berechtigungen erstellen, die den Standardsicherheitsprofilen zugewiesen wurden.

Weitere Informationen erhalten Sie in der Datei "cfcert.ini" (siehe Seite 231) in der Beschreibung des Abschnitts "[Tags]".

Verzeichnissynchronisierungszertifikat

DN:

CN=DSM Directory Synchronisation,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM Directory Synchronisation,O=Computer Associates,C=US

Tag:

dsm_cmdir_eng

Verwendung:

Ermöglicht dem Engine-Job der Verzeichnissynchronisierung die Authentifizierung bei einem Manager.

Zertifikat für allgemeine Server-Registrierung

DN:

CN=DSM Common Server Registration,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM Common Server Registration,O=Computer Associates,C=US

Tag:

dsm_csvr_reg

Verwendung:

Scalability-Server- und Manager-Registrierung zur Authentifizierung bei einem Manager.

CSM-Zertifikat

DN:

CN=Configuration and State Management,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=Configuration and State Management,O=Computer Associates,C=US

Tag:

csm

Verwendung:

Authentifizierung des CSM-Agentencontrollers.

Zertifikat für Mover des Software Delivery-Agenten

DN:

CN=DSM r11 Agent Mover,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM r11 Agent Mover,O=Computer Associates,C=US

Tag:

dsmagtmv

Verwendung:

Mover des Unicenter Software Delivery-Agenten.

Speicherort:

Managerknoten.

Zertifikat für Software Delivery-Katalog

DN:

CN=DSM r11 Software Delivery Catalog,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM r11 Software Delivery Catalog,O=Computer Associates,C=US

Tag:

dsmsdcat

Verwendung:

Software Delivery-Katalog.

Erläuterung:

Manager-Knoten, Agentenknoten (nur Windows).

Hinweise:

- Zertifikat für Software Delivery-Katalog hat Schreibberechtigungen (W) auf Computern und Benutzerprofilen. Das Zertifikat ist auf allen Domänen-Managern und Remote-Engines vorhanden.
- Ändern Sie nicht die Klassenberechtigungen des Computers und des Benutzerprofils eines Zertifikats auf dem Domänen-Manager, und ändern Sie auch nicht die zughörigen Remote-Engines.
- Löschen Sie nicht das standardmäßige oder ein durch den Benutzer angegebenes Software Delivery-Katalogzertifikat mit dem gleichen dsmsdcat-Tag.

Zertifikat für Enterprise-Zugriff

DN:

CN=Enterprise Access,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=Enterprise Access,O=Computer Associates,C=US

Tag:

ent_access

Verwendung:

Kennwortzugriff für Enterprise.

Zertifikat für Domänenzugriff

DN:

CN=Domain Access,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=Domain Access,O=Computer Associates,C=US

Tag:

dom_access

Verwendung:

Kennwortzugriff für Domäne.

Zertifikat für Reporter-Zugriff

DN:

CN=Reporter Access,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=Reporter Access,O=Computer Associates,C=US

Tag:

rep_access

Verwendung:

Kennwortzugriff für Reporter.

Anhang E: Verwendungsbeispiele für die Unterstützung von Sicherheitsbereichen

In diesem Abschnitt werden die wichtigsten Verwendungsbeispiele bezüglich der Bereichsunterstützung aus der Perspektive des Benutzers dargestellt und die Funktionsweise der Bereichsunterstützung erläutert.

Grundlegende Informationen zur Unterstützung der Sicherheitsbereiche und zu Bereichsberechtigungen finden Sie in den Abschnitten Unterstützung der Sicherheitsbereiche (siehe Seite 444) und Bereichsberechtigungen (siehe Seite 427).

Die Beschreibungen der Verwendungsbeispiele sind alle folgendermaßen aufgebaut:

Szenario:

Eine kurze Erläuterung des Benutzerszenarios. Es wird beschrieben, welche Aktionen ein Benutzer durchführen möchte.

Vorbedingungen:

Die Objekte werden definiert, die bereits festgelegt sind, bevor der Benutzer die im Abschnitt "Aktionen" beschriebene Aktion durchführt.

Aktionen:

Die Aktionen des Benutzers werden beschrieben.

Nachbedingungen:

Die Eigenschaften der in einem Szenario verwendeten Objekte, nachdem ein Benutzer die vorherige Aktion ausgeführt hat, werden definiert.

Dieses Kapitel enthält folgende Themen:

Unterstützung von Sicherheitsbereichen für Sicherheitsprofile (siehe Seite 586)
Anwendungsfall: Installieren von CA ITCM (siehe Seite 586)
Anwendungsfall: Aktualisierung einer vorhandenen Installation (siehe Seite 587)
Verwendungsbeispiele: Sicherheitsprofile (siehe Seite 587)
Verwendungsbeispiele: Computer (siehe Seite 589)
Verwendungsbeispiele: Asset-Gruppen (siehe Seite 590)
Verwendungsbeispiele: Abfragen (siehe Seite 595)
Verwendungsbeispiele: Softwarepakete (siehe Seite 597)
Verwendungsbeispiele: Softwareprozeduren (siehe Seite 597)
Verwendungsbeispiele: Softwaregruppen (siehe Seite 598)
Verwendungsbeispiele: Softwarerichtlinien (siehe Seite 599)
Verwendungsbeispiele: Softwarejobs (siehe Seite 599)

Verwendungsbeispiele: Asset-Jobs (siehe Seite 600)
Verwendungsbeispiele: Engine-Tasks (siehe Seite 601)
Verwendungsbeispiele: Verwalten von Bereichen (siehe Seite 601)
Anwendungsfall: Als Eigentum übernehmen (siehe Seite 604)

Unterstützung von Sicherheitsbereichen für Sicherheitsprofile

Die Unterstützung der Sicherheitsbereiche für Sicherheitsprofile erfolgt nach folgenden Regeln:

- Für das Profil "Jeder" kann die Bereichsunterstützung nicht aktiviert oder deaktiviert werden. Der Zugriff auf alle Bereiche wird verweigert.
- Für das Profil "Verteiler" benötigen Sie vollständigen Zugriff auf die Sicherheitsklasse "Unterstützung für Bereich", um die Bereichsunterstützung zu aktivieren oder zu deaktivieren.

Anwendungsfall: Installieren von CA ITCM

Szenario:

Ein Benutzer möchte CA ITCM installieren.

Vorbedingung:

Auf dem Computer ist keine frühere Version von CA ITCM installiert.

Aktion:

Der Benutzer installiert CA ITCM.

Nachbedingungen:

- Standardmäßig integrierte Profile werden installiert.
- Die Unterstützung für den Bereich ist deaktiviert (globale Einstellungen).
- Standardbereichsberechtigungen sind so eingestellt, dass alle Bereiche angezeigt werden.
- Das Profil "Jeder" hat auf keinen Bereich Zugriff.
- Das Profil "Administrator" hat vollständigen Zugriff auf alle Bereicheund kann nicht geändert werden.
- Vordefinierte Bereichsdefinitionen sind nicht installiert.

Anwendungsfall: Aktualisierung einer vorhandenen Installation

Szenario:

Ein Benutzer möchte eine vorhandene Installation aktualisieren.

Vorbedingung:

Der Benutzer hat CA ITCM installiert.

Aktion:

Der Benutzer startet die DSM-MDB-Installation für die Aktualisierung der MDB.

Nachbedingungen:

- Das MDB-Schema wird geändert oder aktualisiert.
- Nach der Installation wird "Bereichsunterstützung" deaktiviert.
- "area_aces" werden für alle vorhandenen gesicherten Objekte erstellt, wobei der Wert wie angegeben in den Standardeinstellungen für den Bereichscode festgelegt wird.

Hinweis: Nach der Aktualisierung sind alle Objekte in allen Bereichen sichtbar. Dies ist die Standardkonfiguration.

Verwendungsbeispiele: Sicherheitsprofile

Die folgenden wichtigen Benutzerszenarien bezüglich Sicherheitsprofilen werden im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen eines Sicherheitsprofils (siehe Seite 588)
- Ändern von Bereichseinstellungen für ein Sicherheitsprofil (siehe Seite 588)
- Löschen eines Sicherheitsprofils (siehe Seite 589)

Anwendungsfall: Erstellen eines Sicherheitsprofils

Szenario:

Ein Administrator möchte ein neues Sicherheitsprofil erstellen.

Vorbedingung:

Das Sicherheitsprofil ist nicht vorhanden.

Aktion:

Der Administrator erstellt das neue Sicherheitsprofil, dem ein oder mehrere Bereichscodes zugewiesen werden.

Nachbedingungen:

- Das Sicherheitsprofil wird erstellt.
- Alle Berechtigungen auf Sicherheitsklassenebene werden für das neue Sicherheitsprofil erstellt.
- Die Berechtigung auf Objektebene wird für alle vorhandenen gesicherten Objekte ermittelt. Die Berechtigungen werden für die vorhandenen gesicherten Objekte ermittelt (einschließlich der Gruppen). Objektberechtigungen werden von der Berechtigung auf Klassenebene abgeleitet.
- Die Bereichsberechtigungen werden erstellt und von den Bereichsberechtigungen abgeleitet, die dem Sicherheitsprofil zugeordnet sind.

Anwendungsfall: Ändern von Bereichseinstellungen für ein Sicherheitsprofil

Szenario:

Ein Administrator möchte den einem Sicherheitsprofil zugewiesenen Bereichscode ändern.

Vorbedingung:

Das Sicherheitsprofil ist vorhanden, und mindestens ein Bereich ist dem Profil zugewiesen.

Aktion:

Der Administrator ändert den Bereichscode für das Sicherheitsprofil, indem er einen neuen Code anlegt.

Nachbedingung:

Die Bereich_ACEs gesicherter Objektewerden nicht geändert.

Anwendungsfall: Löschen eines Sicherheitsprofils

Szenario:

Ein Administrator möchte ein Sicherheitsprofil löschen.

Vorbedingung:

Das Sicherheitsprofil ist vorhanden, und mindestens ein Bereich ist dem Profil zugewiesen.

Aktion:

Der Administrator löscht das Sicherheitsprofil.

Nachbedingungen:

- Das Sicherheitsprofil wird gelöscht.
- Alle Berechtigungsinformationen bezüglich der gesicherten Objekte und der gelöschten Sicherheitsprofile werden ebenfalls gelöscht.

Verwendungsbeispiele: Computer

Die folgenden wichtigen Benutzerszenarien bezüglich Computer werden im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Manuelles Erstellen eines Computers (siehe Seite 589)
- Ein neuer DSM-Agent wurde gefunden (siehe Seite 590)

Anwendungsfall: Manuelles Erstellen eines Computerobjekts

Szenario:

Ein Benutzer möchte ein neues Computerobjekt erstellen.

Vorbedingung:

Der Benutzer ist ein Mitglied eines oder mehrerer Sicherheitsprofile.

Aktion:

Der Benutzer erstellt das neue Computerobjekt mit Hilfe des DSM-Explorers oder des DSM-Befehlszeilen-Hilfsprogramms.

Nachbedingungen:

- Das neue Computerobjekt wird erstellt.
- Der Bereich_ACE wird vom Sicherheitsprofil abgeleitet und dem Computerobjekt zugeordnet. Wenn ein Benutzer Mitglied in mehreren Sicherheitsprofilen ist, werden die Bereich_ACEs aller wichtigen Sicherheitsprofile über die OR-Verknüpfung miteinander verbunden und demgesicherten Objekt zugewiesen.

Anwendungsfall: Ein neuer DSM-Agent wurde gefunden

Szenario:

Ein DSM-Agent wurde bereitgestellt und wird zum ersten Mal ausgeführt.

Vorbedingung:

Für das neue Asset ist kein Objekt in der MDB vorhanden.

Aktion:

Keine Benutzeraktion. Die DSM-Engine erkennt den neuen Agenten und erstellt das Asset-Objekt (wird in ca_discovered_hardware eingefügt).

Nachbedingungen:

- Ein neues gesichertes Objekt wird erstellt.
- Die Bereichsberechtigungen werden wie auf globaler Ebene definiert zugewiesen (globale Konfigurationsparameter).

Verwendungsbeispiele: Asset-Gruppen

Die folgenden wichtigen Benutzerszenarien bezüglich Asset-Gruppen werden im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen einer Asset-Gruppe (siehe Seite 591)
- Hinzufügen eines Computers zu einer Asset-Gruppe (siehe Seite 592)
- Entfernen eines Computers aus einer Asset-Gruppe (siehe Seite 593)
- Ändern der Bereichsberechtigungen einer Asset-Gruppe (siehe Seite 594)
- Deaktivieren der Übernahme und Zurücksetzung (siehe Seite 594)

Anwendungsfall: Erstellen einer Asset-Gruppe

Szenario:

Ein Benutzer möchte eine neue Asset-Gruppe erstellen, in der der Benutzer Mitglied nur eines Sicherheitsprofils ist.

Vorbedingung:

Eine Gruppe mit demselben Namen ist noch nicht vorhanden.

Aktion:

Der Benutzer erstellt die neue Asset-Gruppe.

Nachbedingungen:

- Die neue Gruppe wird erstellt.
- Ein Gruppen_ACE wird basierend auf den Berechtigungen auf Klassenebene für Gruppen erstellt.
- Ein Objekt_ACE wird basierend auf den Berechtigungen auf Klassenebene für Gruppen erstellt.
- Der Bereich_ACE wird aus dem Sicherheitsprofil erfasst, zu dem der Erstellungsbenutzer gehört. Wenn der Erstellungsbenutzer unbekannt ist, wird der standardmäßige Bereich_ACE verwendet.

Hinweis: Dasselbe gilt für Scalability-Servergruppen und Domänengruppen.

Anwendungsfall: Hinzufügen eines Computers zu einer Asset-Gruppe

Szenario:

Ein Benutzer möchte einen Computer einer Gruppe hinzufügen, in der der Benutzer Mitglied in nur einem Sicherheitsprofil ist.

Vorbedingungen:

- Die Asset-Gruppe ist vorhanden.
- Der Computer ist vorhanden.

Aktion:

Der Benutzer fügt einen Computer einer Gruppe hinzu. Übernahme ist für die Gruppe aktiviert.

Nachbedingungen:

- Der Computer ist mit der Gruppe verknüpft.
- Falls es sich nicht um eine Übernahmegruppe handelt, wird keine Aktion ausgeführt. Falls es sich um eine Übernahmegruppe handelt, wird der Objekt_ACE basierend auf dem Objekt_ACE der übergeordneten Gruppe ermittelt.
- Der Bereichscode wird folgendermaßen festgelegt:
  - Wenn der Computer nur Mitglied in einer Asset-Gruppe ist, ist der Bereich_ACE mit dem Bereich_ACE der Asset-Gruppe identisch.
  - Wenn der Computer Mitglied in mehreren Asset-Gruppen ist, werden die Bereich_ACEs der übergeordneten Gruppen über die OR-Verknüpfung miteinander verbunden und dem gesicherten Objekt zugewiesen.

Varianten:

Wenn vor dem Hinzufügen zur Gruppe für die Bereichsberechtigung des Computers die Ebene des Erstellungsbenutzers oder die globale Standardebene festegelegt wird, werden die Bereichsberechtigungen der Gruppe für die Bereichsberechtigung eingestellt.

Wenn vor dem Hinzufügen zur Gruppe für die Bereichsberechtigung des Computers die Objektebene festegelegt wird, werden die Bereichsberechtigungen nicht auf der Gruppenebene festgelegt. Der Benutzer muss die Funktion "ZURÜCKSETZEN" verwenden, um die Bereichsberechtigungen erneut zu berechnen, um mit der Gruppe konform zu sein.

Bereichsberechtigungen dürfen nicht geändert werden, wenn die Berechtigungsübernahme deaktiviert ist.

Hinweis: Dasselbe gilt im Falle einer dynamischen Gruppe und der Engine, die die Gruppenevaluierung durchführt. In diesem Fall wird das Mitglied durch die Engine mit der Gruppe verknüpft.

Anwendungsfall: Entfernen eines Computers aus einer Asset-Gruppe

Szenario:

Ein Benutzer möchte einen Computer aus einer Asset-Gruppe entfernen, in der der Benutzer Mitglied eines oder mehrerer Sicherheitsprofile ist.

Vorbedingungen:

- Die Asset-Gruppe ist vorhanden.
- Der Computer ist vorhanden.
- Der Computer ist Mitglied in nur einer Asset-Gruppe.

Aktion:

Der Benutzer entfernt die Verknüpfung des Computers mit der Asset-Gruppe. Übernahme ist für die Gruppe aktiviert.

Nachbedingungen:

- Die Verknüpfung des Computers mit der Gruppe wird entfernt.
- Bereichsberechtigungen werden nicht aktualisiert.
- Als Sicherheitsebene ist die Objektebene eingestellt.

Varianten:

Wenn der Computer Mitglied mehrerer Asset-Gruppen ist und als Sicherheitsebene die Gruppenebene eingestellt ist, werden die Bereichsberechtigungen erneut berechnet (basierend auf der verbleibenden Gruppenzuweisung)und aktualisiert.

Wenn für die Bereichsberechtigung die Objektebene festgelegt wird, wird die Bereichsberechtigung nicht aktualisiert.

Hinweis: Nachdem der Computer aus der Asset-Gruppe entfernt wurde, kann der Benutzer die Funktion "ZURÜCKSETZEN" verwenden, um die Bereichsberechtigungen des Computers auf der Erstellungsbenutzerebene festzulegen.

Anwendungsfall: Ändern der Bereichsberechtigung einer Asset-Gruppe

Szenario:

Ein Benutzer möchte die Bereichsberechtigungen einer vorhandenen Asset-Gruppe ändern.

Vorbedingungen:

- Der Benutzer ist mit mindestens einem Sicherheitsprofil verknüpft.
- Die Asset-Gruppe ist vorhanden, wo die Berechtigungsvererbung aktiviert wird.

Aktion:

Der Benutzer verwendet das Dialogfeld "Berechtigungen ändern" und verknüpft mindestens einen Bereich mit der vorhandenen Gruppe bzw. hebt die Verknüpfung auf.

Nachbedingungen:

- Das "area_ace" der vorhandenen Gruppe wird geändert.
- Wenn es eine Vererbungsgruppe ist, wird das "area_ace" der Mitglieder aktualisiert.

Hinweis: Das Aktivieren und Deaktivieren der Berechtigungsvererbung ändert nicht die Bereichsberechtigungen.

Anwendungsfall: Deaktivieren der Übernahme und Zurücksetzung

Szenario:

Ein Benutzer möchte die Übernahme einer Asset-Gruppe deaktivieren und eine Zurücksetzung auf Asset-Ebene durchführen.

Vorbedingungen:

- Eine Asset-Gruppe mit aktivierter Berechtigungsübernahme ist vorhanden.
- Ein Computer ist mit der Asset-Gruppe verbunden, in der die Bereichsberechtigungen zum Zeitpunkt der Verknüpfung auf der Objektebene festgelegt werden.

Aktion:

Der Benutzer deaktiviert die Berechtigungsübernahme der Asset-Gruppe und führt eine "Zurücksetzung" für das Computerobjekt durch.

Nachbedingung:

Die Objektberechtigungen des Computers werden auf den Erstellungsbenutzer zurückgesetzt.

Hinweis: Durch Aktivieren und Deaktivieren der Berechtigungsübernahme werden die Bereichsberechtigungen nicht geändert.

Verwendungsbeispiele: Abfragen

Die folgenden wichtigen Benutzerszenarien bezüglich Abfragen werden im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen einer Abfrage (siehe Seite 595)
- Ausführen einer Abfrage (siehe Seite 596)
- Ausführen einer Abfrage im Kontext von Software Delivery (siehe Seite 596)

Anwendungsfall: Erstellen einer Abfrage

Szenario:

Ein Benutzer möchte eine neue Abfrage erstellen.

Vorbedingung:

Der Benutzer ist Mitglied nur eines Sicherheitsprofils.

Aktion:

Der Benutzer erstellt die neue Abfrage.

Nachbedingungen:

- Die neue Abfrage wird erstellt.
- Der Bereich_ACE der Abfrage wird vom Profil des Erstellungsbenutzers der Abfrage abgeleitet.
- Die neue Abfrage enthält eine zusätzliche 'where'-Bedingung, mit der sichergestellt wird, dass die Abfrage nur Objekte zurückgibt, auf die der Erstellungsbenutzer Zugriff hat (derselbe Bereich_ACE, der der Abfrage zugewiesen ist).
- Der Objekt_ACE wird basierend auf dem sich auf Klassenebene befindenden ACE der Sicherheitsklasse für Abfragen erstellt.

Anwendungsfall: Ausführen einer Abfrage

Szenario:

Ein Benutzer möchte eine dynamische Computergruppe erstellen. Die Gruppe muss durch die Engine evaluiert werden.

Vorbedingung:

Keine

Aktion:

Ein Benutzer erstellt eine dynamische Gruppe. Die übergeordnete Gruppe ist "Alle Computer".

Die Abfragewurde von einem anderen Benutzer erstellt als die Gruppe.

Nachbedingungen:

Die Evaluierung der Gruppe wird von der Engine basierend auf folgenden Regeln durchgeführt:

- Die Abfrage wird ausgeführt.
- Es werden nur die Computer als Gruppenmitglieder hinzugefügt, die in denselben Bereich fallen wie der Benutzer, der die Gruppe erstellt hat.

Das bedeutet, dass die Bereichsberechtigungen der Gruppe eine höhere Priorität haben als die Bereichsberechtigungen der Gruppe.

Anwendungsfall: Ausführen einer Abfrage im Kontext von Software Delivery

Szenario:

Eine Abfrage wird als Teil einer Software Delivery-Prozedurvoraussetzung evaluiert. Die Evaluierung wird vom Task-Manager von Software Delivery ausgeführt.

Vorbedingung:

Eine Prozedur mit einer Voraussetzung wird für eine Installation auf einem Zielcomputer verwendet, und die globale Bereichseinstellung ist aktiviert.

Aktion:

Der Task-Manager ruft die Abfrageevaluierungs-API auf und übermittelt den Benutzer aus dem Software Delivery-Aktivitätsobjekt.

Nachbedingung:

Die Abfrage wird im selben Kontext evaluiert wie der Benutzer, der den Job in der GUI erstellt hat. Das bedeutet, das die Abfrage nur Objekte in dem Bereich zurückgibt, in dem sich der Benutzer, der den Job erstellt hat, befindet. Wenn der Job mit Hilfe eines Hintergrundprozesses erstellt wurde, in dem kein Benutzerkontext verfügbar war, gibt die Abfragenevaluierung alle Objekte wie bei nicht aktivierter Bereichsunterstützung zurück.

Verwendungsbeispiele: Softwarepakete

Das folgende wichtige Benutzerszenario bezüglich Softwarepaketen wird im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen eines Softwarepakets (siehe Seite 597)

Anwendungsfall: Erstellen von Softwarepaketen

Szenario:

Ein Benutzer möchte ein neues Softwarepaket erstellen.

Vorbedingung:

Das Softwarepaket war nicht vorhanden.

Aktion:

Der Benutzer erstellt das Softwarepaket mit Hilfe der CA ITCM-GUI.

Nachbedingungen:

- Das Softwarepaket wird erstellt.
- Bereichsberechtigungen werdenerstellt, und das Softwarepaket wird mit denselben Bereichen verknüpft, mit denen der Benutzer verknüpft ist, der das Objekt erstellte.

Verwendungsbeispiele: Softwareprozeduren

Das folgende wichtige Benutzerszenario bezüglich Softwareprozeduren wird im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen einer Softwareprozedur (siehe Seite 598)

Anwendungsfall: Erstellen einer Softwareprozedur

Szenario:

Ein Benutzer möchte eine neue Softwareprozedur erstellen.

Vorbedingung:

Die Softwareprozedur war nicht vorhanden.

Aktion:

Der Benutzer erstellt die Softwareprozedur mit Hilfe der CA ITCM-GUI.

Nachbedingung:

Die Prozedur "übernimmt" die Bereichsberechtigungen des Softwarepakets, in dem sie enthalten ist.

Verwendungsbeispiele: Softwaregruppen

Das folgende wichtige Benutzerszenario bezüglich Softwaregruppen wird im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen einer Softwaregruppe (siehe Seite 598)

Anwendungsfall: Erstellen einer Softwaregruppe

Szenario:

Ein Benutzer möchte eine neue Softwaregruppe erstellen.

Vorbedingung:

Der Benutzer ist ein Mitglied eines oder mehrerer Sicherheitsprofile.

Aktion:

Der Benutzer erstellt die neue Softwaregruppe mit Hilfe des DSM-Explorers (ein neuer Knoten unter der Softwarepaketbibliothek).

Nachbedingungen:

- Die neue Softwaregruppe wird erstellt.
- Der Bereich_ACE der Softwaregruppe wird vom Profil des Erstellungsbenutzers der Abfrage abgeleitet.
- Der Objekt_ACE wird basierend auf dem sich auf Klassenebene befindenden ACE der Sicherheitsklasse für Asset-Jobs erstellt.
- Ein Gruppen_ACE wird ebenfalls basierend auf dem sich auf Klassenebene befindenden ACE des Sicherheitsprofils erstellt.

Verwendungsbeispiele: Softwarerichtlinien

Das folgende wichtige Benutzerszenario bezüglich Softwarerichtlinien wird im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen einer Softwarerichtlinie (siehe Seite 599)

Anwendungsfall: Erstellen einer Softwarerichtlinie

Szenario:

Ein Benutzer möchte eine neue Softwarerichtlinie erstellen.

Vorbedingung:

Der Benutzer ist ein Mitglied eines oder mehrerer Sicherheitsprofile.

Aktion:

Der Benutzer erstellt die neue Softwarerichtlinie mit Hilfe des DSM-Explorers oder der CA ITCM-Befehlszeile.

Nachbedingungen:

- Die neue Softwarerichtlinie wird erstellt.
- Die Softwarerichtlinie wird einer Richtliniengruppe zugewiesen.
- Der Objekt_ACE wird vom ACE zum Auswählen der Klasse abgeleitet.
- Die Bereichsberechtigungen der Software-Richtlinie werden vom Profil des Erstellungsbenutzers der Richtlinie abgeleitet.

Verwendungsbeispiele: Softwarejobs

Das folgende wichtige Benutzerszenario bezüglich Softwarejobs wird im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen eines Softwarejobs (siehe Seite 600)

Anwendungsfall: Erstellen von Softwarejobs

Szenario:

Ein Benutzer möchte einen neuen Softwarejob erstellen.

Vorbedingung:

Der Benutzer ist ein Mitglied eines oder mehrerer Sicherheitsprofile.

Aktion:

Der Benutzer erstellt den neuen Software-Job mit Hilfe des DSM-Explorers oder der DSM-Befehlszeile.

Nachbedingungen:

- Der neue Softwarejob wird erstellt.
- Objektberechtigungen werden vom ACE zum Auswählen der Klasse abgeleitet
- Die Bereichsberechtigungen des Software-Jobs werden vom Profil des Erstellungsbenutzers des Jobs abgeleitet.

Verwendungsbeispiele: Asset-Jobs

Das folgende wichtige Benutzerszenario bezüglich Asset-Jobs wird im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen eines Asset-Jobs (siehe Seite 600)

Anwendungsfall: Erstellen eines Asset-Jobs

Szenario:

Ein Benutzer möchte einen neuen Asset-Job erstellen.

Vorbedingung:

Der Benutzer ist Mitglied nur eines Sicherheitsprofils.

Aktion:

Der Benutzer erstellt den neuen Asset-Job. Der Asset-Job kann jeglichen Jobtyps sein, wie beispielsweise Meldungen, Befehl usw.

Nachbedingungen:

- Der neue Asset-Job wird erstellt.
- Der Bereich_ACE des Asset-Jobs wird vom Profil des Erstellungsbenutzers der Abfrage abgeleitet.
- Der Objekt_ACE wird basierend auf dem sich auf Klassenebene befindenden ACE der Sicherheitsklasse für Asset-Jobs erstellt.

Verwendungsbeispiele: Engine-Tasks

Das folgende wichtige Benutzerszenario bezüglich Engine-Tasks wird im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstellen eines Engine-Tasks (siehe Seite 601)

Anwendungsfall: Erstellen eines Engine-Tasks

Szenario:

Ein Benutzer möchte einen neuen Engine-Task erstellen.

Vorbedingung:

Der Benutzer ist Mitglied nur eines Sicherheitsprofils.

Aktion:

Der Benutzer erstellt den neuen Engine-Task.

Nachbedingungen:

- Der neue Engine-Task wird erstellt.
- Die Bereichsberechtigung des Engine-Tasks wird vom Profil des Erstellungsbenutzers des Engine-Tasks abgeleitet.
- Die Objektberechtigungen werden basierend auf den sich auf Klassenebene befindenden Berechtigungen der Sicherheitsklasse für Ressourcenjobs erstellt.

Verwendungsbeispiele: Verwalten von Bereichen

Die folgenden wichtigen Benutzerszenarien bezüglich der Verwaltung von Bereichen werden im Rahmen der Unterstützung der Sicherheitsbereiche behandelt:

- Erstmaliges Aktivieren der Bereichscodeunterstützung (siehe Seite 602)
- Deaktivieren der Bereichscodeunterstützung (siehe Seite 602)
- Erneutes Aktivieren der Bereichscodeunterstützung (siehe Seite 603)
- Ändern der Standardbereichsberechtigungen (siehe Seite 603)
- Hinzufügen eines neuen Bereichs (siehe Seite 604)
- Löschen eines Bereichs (siehe Seite 604)

Anwendungsfall: Erstmaliges Aktivieren der Bereichscodeunterstützung

Szenario:

Ein Administrator möchte den Bereichscode für alle Sicherheitsprofile aktivieren. Zuvor war er deaktiviert.

Vorbedingungen:

- Die Bereichscodeunterstützung ist deaktiviert, und das CA ITCM-Produkt wurde bereits verwendet.
- Gesicherte Objekte und Profile wurden erstellt, während die Bereichsunterstützung deaktiviert war.

Aktion:

Der Administrator aktiviert die Bereichscodeunterstützung.

Nachbedingungen:

- Die Bereichscodeunterstützung wird in der MDB aktiviert.
- Die Bereichscodes aller Profile werden auf den Standardbereichscode eingestellt, der bei der Erstellung des Sicherheitsprofils definiert wurde.
- Die Bereichscodes für die vorhandenen gesicherten Objekte werden auf die Bereichscodes eingestellt, die für das Sicherheitsprofil definiert wurden.

Hinweis: Dies bedeutet, dass ein Administrator dem Sicherheitsprofil explizit einen oder mehrere Bereichscodes zuweisen muss, nachdem er die Bereichscodeunterstützung zum ersten Mal aktiviert hat.

Anwendungsfall: Deaktivieren der Bereichscodeunterstützung

Szenario:

Ein Administrator möchte die Bereichscodes für alle Sicherheitsprofile deaktivieren.

Vorbedingung:

Die Bereichscodes sind in der MDB richtig festgelegt.

Aktion:

Der Administrator deaktiviert die Bereichscodeunterstützung.

Nachbedingungen:

- Das Flag in der MDB wird so festgelegt, dass der Bereichscode deaktiviert wird.
- Der Bereichscode selbst wird weder gelöscht noch geändert.

Anwendungsfall: Erneutes Aktivieren der Bereichscodeunterstützung

Szenario:

Ein Administrator möchte den Bereichscode für alle Sicherheitsprofile wieder aktivieren.

Vorbedingung:

Die Bereichscodes sind in der MDB richtig festgelegt, die Bereichscodeunterstützung ist jedoch deaktiviert.

Aktion:

Der Administrator aktiviert die Bereichscodeunterstützung.

Nachbedingungen:

- Das Flag in der MDB wird so festgelegt, dass der Bereichscode aktiviert wird.
- Der Bereichscode selbst ist derselbe wie vor der Deaktivierung der Bereichscodeunterstützung.

Anwendungsfall: Ändern der Standardbereichsberechtigungen

Szenario:

Ein Benutzer möchte die Standardbereichsberechtigungen ändern.

Vorbedingung:

Der Benutzer hat CA ITCM installiert.

Aktion:

Der Benutzer ändert die Standardberechtigungen.

Nachbedingungen:

- Die wie in der MDB gespeicherten Standardbereichsberechtigungen werden geändert.
- Alle Bereichsberechtigungen, wo die Sicherheitsstufe auf "Standardwert" festgelegt wird, werden auch geändert.

Anwendungsfall: Hinzufügen eines neuen Bereichs

Szenario:

Ein Benutzer möchte eine neue Bereichsdefinition erstellen.

Vorbedingung:

Der Benutzer ist Mitglied eines Sicherheitsprofils. Die Sicherheitsklasse zur Steuerung der Bereichsunterstützung (SEC_CLSID_COM_CONTROL_AREA) lässt mindestens die Erstellung eines neuen Bereichs zu.

Aktion:

Der Benutzererstellt die neue Bereichsdefinition.

Nachbedingung:

Der neue Bereichwird erstellt.

Anwendungsfall: Löschen eines Bereichs

Szenario:

Ein Benutzer möchte eine Bereichsdefinition löschen.

Vorbedingung:

Der Benutzer ist Mitglied eines Sicherheitsprofils. Die Sicherheitsklasse zur Steuerung der Bereichsunterstützung (SEC_CLSID_COM_CONTROL_AREA) lässt mindestens das Löschen eines Bereichs zu.

Aktion:

Der Benutzer löscht die Bereichsdefinition manuell.

Nachbedingungen:

- Der Bereichwird gelöscht.
- Bereichsberechtigungen werden so aktualisiert, dass der Bereich nicht mehr vorhanden ist.

Anwendungsfall: Als Eigentum übernehmen

Durch die Berechtigung "Als Eigentum übernehmen" wird die Bereichsberechtigung für Objekte nicht geändert.

Anhang F: CAF Geplante Jobs

Im Folgenden werden die vollständigen Regeln für die Festlegung geplanter Jobs, die im Common Application Framework (CAF) ausgeführt werden, beschrieben. Zu diesen Jobs gehört das Ausführen von caf-Befehlen in regelmäßigen oder zufälligen Intervallen. Es gibt beispielsweise einen Standardjob, der den Asset Management-Agenten ein Mal pro Tag ausführt.

Dieses Kapitel enthält folgende Themen:

CAF-Standardjobs und -parameter (siehe Seite 605)
Beispiele für geplante CAF-Jobs (siehe Seite 608)

CAF-Standardjobs und -parameter

CAF wird mit einer Reihe von Standardjobs installiert (weitere Informationen finden Sie in der *DSM-Explorer-Hilfe* im Abschnitt "Konfigurationsrichtlinie" unter "Richtliniengruppe 'CAF'").

Ein Job wird durch einen Parametersatz beschrieben, der im Konfigurationsspeicher (comstore) unter folgendem Schlüssel gespeichert ist:

`itrm/common/caf/scheduler/`*`name_des_jobs`*

Der Scheduler selbst kann durch Einstellen des Parameters "enabled" im obigen Schlüssel aktiviert oder deaktiviert werden.

Es gibt folgende Parameter eines Jobs:

desc

Legt die Jobbeschreibung fest; diese wird in Trace-Protokollen angezeigt.

enabled

Zeigt an, ob ein Job aktiviert ist. Gültige Werte sind: 1 = Job ist aktiviert, 0 = Job ist deaktiviert und wird nicht ausgeführt.

type

Gibt den Typ des Jobs an. Damit wird der zeitliche Rahmen festgelegt, in dem sich der Job wiederholt. Folgende Werte sind möglich:

Tag

Führt den Job im Abstand von einigen Tagen zu einer bestimmten Uhrzeit aus.

hour

Führt den Job im Abstand von einigen Stunden in einer bestimmten Minute der Stunde aus.

minute

Führt den Job im Abstand von einigen Minuten aus.

Sie können auch folgende zusätzliche Schlüsselwörter angeben:

now

Führt den Job jetzt und anschließend in den angegebenen Intervallen aus. Das Wort "jetzt" in diesem Kontext bedeutet "beim Start von caf".

Wenn der Parameter "randomnowtime" eingestellt ist, wird der Job innerhalb einer zufälligen Anzahl von Sekunden bis zum Wert von "randomnowtime" ausgeführt. Auf diese Weise wird sichergestellt, dass Computer beim gemeinsamen Start nicht alle ihre Jobs gleichzeitig auslösen.

random

Führt den Job zu einer angegebenen Zeit plus einer zufälligen Anzahl an Minuten bis zu dem Wert des Parameters "randomminutes" aus. Dies wird bei Jobs verwendet, bei denen die Herstellung von Verbindungen zu Servern eingeschlossen ist. Auf diese Weise wird die Belastung für Server verteilt, indem teilweise eine zufällige Zeit angegeben wird, zu der die Agenten Kontakte herstellen.

random_hour

Gibt an, dass der Job zu einer zufälligen Stunde des Tages ausgeführt wird. Wird bei täglichen Zeitplänen verwendet.

random_minute

Gibt an, dass der Job zu einer zufälligen Minute einer Stunde (die ebenfalls zufällig sein kann) ausgeführt wird. Wird bei täglichen und stündlichen Zeitplänen verwendet.

excludeDays

Gibt die Namen der Tage an, die aus dem Zeitplan entfernt werden sollen: "monday" (Montag), "tuesday" (Dienstag) usw. Trennen Sie die Tage durch Leerzeichen. Zum Beispiel verhindert die Einstellung "monday wednesday", dass der Job am Montag und am Mittwoch ausgeführt wird.

excludeHours

Gibt im 24-Stunden-Format die Anzahl der Stunden an, die aus dem Zeitplan entfernt werden sollen. Trennen Sie die Stunden durch Leerzeichen. Zum Beispiel verhindert die Einstellung "1 15", dass der Job um 1:00 Uhr und um 15:00 Uhr ausgeführt wird.

hour

Gibt die Startzeit des Jobs im 24-Stunden-Format an. Dies wird nur mit täglichen Zeitplänen verwendet.

minute

Gibt die Minute der Stunde an, in der der Job gestartet wird. Dies wird mit täglichen und stündlichen Zeitplänen verwendet.

repeat

Wiederholt jede mit der Eigenschaft "type" definierte Zeiteinheit. Wenn der Typ beispielsweise "hour" ist, legt "repeat" die Anzahl der Stunden zwischen den Jobs fest.

randomnowtime

Gibt eine Sekundenzahl an. Wenn CAF startet, wird ein als "now" markierter Job zu einer zufälligen Uhrzeit innerhalb dieser Anzahl von Sekunden ausgeführt.

randomminutes

Gibt eine Minutenzahl an. Der Job wird zu einer angegebenen Zeit plus einer zufälligen Zeit bis zu dem Wert dieses Parameters ausgeführt.

cmd

Gibt den caf-Befehl zur Ausführung des Jobs an. Dieser ist mit der Befehlszeile identisch, mit der Ausnahme, dass die Optionen "host", "user" und "password" nicht verwendet werden können.

Beispiele für geplante CAF-Jobs

Beispiel: Das Plugin "amagent" soll stündlich zu jeder vollen Stunde ausgeführt werden.

```
type=”hour”, repeat=1, minute=0, cmd=”start amagent”
```

Beispiel: Das Plugin "amagent" soll jeden Tag um 14:30 Uhr ausgeführt werden.

```
type = "day", repeat = 1, hour = 14, minute = 30, cmd = "start amagent"
```

Beispiel: Das Plugin "amagent" soll ausgeführt werden, wenn CAF gestartet wird, und danach jeden Tag zu einer zufälligen Zeit zwischen 1:00 Uhr und 2:30 Uhr, außer am Wochenende.

```
type="day now random", hour=1, minute=0, randomminutes=90, excludedays="saturday
sunday", cmd=" start amagent"
```

Anhang G: FIPS 140-2-Konformität

In diesem Anhang werden Details zur Kryptographie-Verwendung CA ITCM erklärt, insbesondere zum Konformitäts-Level mit den Standards der FIPS 140-2-Veröffentlichung.

Dieses Kapitel enthält folgende Themen:

FIPS PUB 140-2 (siehe Seite 609)
Referenzen (siehe Seite 610)
Unterstützte FIPS-Modi (siehe Seite 610)
Kryptographisches Modul – RSA Crypto (siehe Seite 611)
Kryptographische Sicherheitsfunktionen (siehe Seite 611)
Komponentenspezifische Verwendung von Kryptographie (siehe Seite 613)
FIPS-Konformität von CA ITCM-externen Komponenten (siehe Seite 614)
Nicht genehmigte Verwendung von Sicherheitsfunktionen (siehe Seite 616)

FIPS PUB 140-2

FIPS 140-2 ist ein Sicherheitsstandard, der die Sicherheitsanforderungen für ein kryptographisches Modul, das innerhalb eines Sicherheitssystems verwendet wird, festlegt. Dieser Standard, der von NIST zur Verfügung gestellt wird, dient der Bewertung und Anerkennung der Vorgänge von kryptographischen Modulen durch das Cryptographic Module Verification Program (CMVP). CMVP wird von durch NIST anerkannte Testlabors ausgeführt, um kryptographische Module zu testen und zu validieren. Im Test werden die Module mit den vom FIPS 140-2-Standard abgeleiteten Testanforderungen verglichen.

Für jede Sicherheitsfunktion, die für die Verwendung im FIPS 140-2-genehmigten Modus validiert und genehmigt wurde, wird im FIPS 140-2-Genehmigungsszertifikat für das Modul ein individuelles Zertifikat unter Cryptographic Algorithm Validation Program (CAVP) gespeichert. Im Genehmigungszertifikat werden alle im Modul verfügbaren Sicherheitsfunktionen aufgelistet (sowohl genehmigte als auch nicht genehmigte Funktionen), und jene Funktionen beschrieben, die im FIPS 140-2-genehmigten Betriebsmodus verwendet werden können.

Jedes genehmigte Modul veröffentlicht ein verknüpftes Sicherheitsrichtliniendokument, das beschreibt, auf welche Weise das Modul verwendet werden muss, um mit dem FIPS 140-2-Standard konform zu sein.

Hinweis: Es können nur kryptographische Module als durch FIPS 140-2 akredidiert und genehmigt zertifiziert werden. Für Anwendungen ist diese Zertifizierung nicht möglich, doch sie können in ihren entsprechenden genehmigten Betriebsmodi FIPS 140-2-genehmigte Module verwenden.

Referenzen

Weitere Informationen zu Cryptographic Module Verification Program finden Sie auf Website von NIST:

http://csrc.nist.gov/groups/STM/cmvp/

Unter der folgenden URL werden die validierten Module einschließlich Verknüpfungen zu den relevanten Sicherheitsrichtlinien angezeigt:

http://csrc.nist.gov/groups/STM/cmvp/validation.html

Unter der angeführten URL finden Sie auch Informationen zu den Zertifikatsnummern, auf die in diesem Anhang Bezug genommen wird.

Unterstützte FIPS-Modi

CA ITCM kann in einem der folgenden Modi betrieben werden:

FIPS-bevorzugt

Im FIPS-bevorzugten Modus zieht CA ITCM FIPS 140-2-genehmigte Sicherheitsfunktionen vor. Bei der Kommunikation mit Legacy-CA ITCM-Komponenten werden jedoch Legacy-Sicherheitsfunktionen verwendet. Die eingebetteten kryptographischen Module werden in diesem Modus *nicht* in FIPS 140-2-genehmigten Modi verwendet, da sie die Verwendung von nicht genehmigten Sicherheitsfunktionen wie z. B. MD5 erforderlich machen. Im FIPS-bevorzugten Modus ist die Kommunikation und Interaktion von CA ITCM mit früheren Versionen von CA ITCM möglich.

Nur-FIPS

Im Nur-FIPS-Modus verwendet CA ITCM *nur* FIPS 140-2-genehmigte Sicherheitsfunktionen. Wie in den folgenden Kapiteln beschrieben, existieren nicht kryptographische Verwendungen von nicht genehmigten Sicherheitsfunktionen. In einem FIPS 140-2-genehmigten Betriebsmodus werden sie jedoch nicht durch eingebettete kryptographische Module zur Verfügung gestellt. In diesem Modus kann CA ITCM nur mit Komponenten interagieren, die entweder im FIPS-bevorzugten oder im Nur-FIPS-Modus FIPS-konform sind.

Hinweis: Dieser Anhang konzentriert sich auf die Verwendung von Kryptographie im Nur-FIPS-Modus.

Kryptographisches Modul – RSA Crypto

Die folgenden kryptographischen Module werden von CA ITCM direkt verwendet und eingebettet:

- RSA Crypto-C ME Version 2.1; CMVP-Zertifikat #828

Nachstehend finden Sie einen Auszug aus der Sicherheitsrichtlinie für dieses kryptographische Modul:

"Dieses kryptographische Modul ist als eigenständiges, FIPS 140-2-geeignetes Multi-Chip-Modul klassifiziert. Als solches muss es unter einem bestimmten Betriebssystem und auf einer bestimmten Computerplattform getestet werden. Infolgedessen beinhaltet die kryptographische Begrenzung die Ausführung des kryptographischen Moduls im auf ausgewählten Plattformen und unter ausgewählten Betriebssystemen, wenn es im Einzelbenutzermodus konfiguriert ist. Das kryptographische Modul wurde als konform mit allen FIPS 140-2 Level 1-Sicherheitsanforderungen, einschließlich kryptographischer Schlüsselverwaltung und Betriebssystemanforderungen, validiert. Das kryptographische Modul ist gepackt als dynamisch geladenes Modul oder freigegebene Bibliotheksdatei, die alle ausführbaren Codes des Moduls enthalten. Zusätzlich stützt sich das RSA BSAFE Crypto-C ME-Hilfsprogramm auf die physische Sicherheit des Host-PCs, auf dem es ausgeführt wird."

Kryptographische Sicherheitsfunktionen

Die folgende Tabelle beinhaltet die kryptographischen Algorithmen des RSA Crypto-C-Moduls, die für verschiedene CA ITCM-Sicherheitsfunktionen verwendet werden:

Sicherheitsfunktion	**Kryptoalgorithmus**	**Validierungszertifikat-Nr.**	**Kommentare**
Asymmetrische Verschlüsselung und Entschlüsselung	RSA-Verschlüsselung und -Entschlüsselung	Nicht genehmigt	Im FIPS 140-2-Modus für Schlüsseltransport genehmigt
Symmetrische Verschlüsselung und Entschlüsselung	AES CBC	490	FIPS PUB 197 – Advanced Encryption Standard
	Triple-DES	510	FIPS PUB 46-3 - Datenverschlüsselungs-Standards FIPS SP 800-67 - Empfohlen für Triple Data Encryption Algorithm (TDEA) Block Cipher ANSI X9.52 – TDEA-genehmigte Betriebsmodi

Sicherheitsfunktion	**Kryptoalgorithmus**	**Validierungszertifikat-Nr.**	**Kommentare**
Hashfunktionen	SHA-1	560	FIPS PUB 180-3 – Sicherer Hash-Standard
	SHA-256	560	FIPS PUB 180-3 – Sicherer Hash-Standard
	SHA-512	560	FIPS PUB 180-3 – Sicherer Hash-Standard
Zufallszahlengenerierung	PRNG	270	FIPS PUB 186-2 – Digital Signature Standard Weitere Informationen finden Sie im Anhang 3 ("Random Number Generation") des FIPS PUB 186-2 Digital Signature Standard-Dokuments.
Asymmetrische Schlüsselerstellung	TLS 1.0	Nicht zutreffend	Im FIPS 140-2 Implementation Guidance-Dokument für FIPS-genehmigte Cipher-Suites erlaubt.
	SSH v2	Nicht zutreffend	Im FIPS 140-2 Implementation Guidance-Dokument für FIPS-genehmigte Cipher-Suites erlaubt.

Komponentenspezifische Verwendung von Kryptographie

In diesem Abschnitt wird die komponentenspezifische bei CA ITCM-Betrieb im Nur-FIPS-Modus aufgelistet:

Kommunikation zwischen Knoten [Session Messaging]

Die Session Messaging-Komponente verwendet für die Kommunikation zwischen Knoten das TLS v1.0-Protokoll. Die Cipher-Suite wird durch die Übertragung zwischen den kommunizierenden Knoten ausgewählt.

In einigen Instanzen verwendet die Session Messaging-Komponente die Struktur der Schlüsseltransport-Empfängerinformationen gemäß Version 3 des Cryptographic Message Syntax (CMS3), festgelegt in RFC3369.

Stream-basiertes Netzwerk

Die Stream-basierte Netzwerk-Komponente verwendet für die Kommunikation zwischen Knoten das TLS v1.0-Protokoll. Die Cipher-Suite wird durch die Übertragung zwischen den kommunizierenden Knoten ausgewählt.

Remote Control - Lokales Adressbuch

Die Einträge ins lokale Remote Control-Adressbuch sind durch den 3TDES-Algorithmus im CBC-Modus mit zufallsgeneriertem IV geschützt.

Desktop Migration Manager [DMM]

DMM verwendet das TLS v1.0-Kommunikationsprotokoll, sowie des AES-Algorithmus mit einer Schlüssellänge von 192 Bit im CBC-Modus mit zufallsgeneriertem IV.

ENC

Da CA ITCM derzeit mit einer ENC-Funktion nur für Windows geliefert wird, ist diese fest mit dem Microsoft SCHANNEL-Provider; dem Zertifikatsspeicher von Microsoft, integriert und unterliegt dem Microsoft-Kryptographieanbieter (RSAENH). Weitere Informationen zum FIPS-Status des Kryptographieanbieters von Microsoft finden Sie in FIPS-zertifizierte Windows-Betriebsumgebungen (siehe Seite 615).

OSIM und Software Delivery

OSIM und Software Delivery verwenden vom AES-Algorithmus zur Verfügung gestellte symmetrische Verschlüsselung im CBC-Modus mit zufallsgeneriertem IV und einer Struktur, die die Version 3 des Cryptographic Message Syntax (CMS3), festgelegt in RFC3369, verwendet.

Common Object-Manager, Allgemeine Engine, SMS Extractor

Die Komponenten des Common Object-Managers, der allgemeinen Engine und des SMS Extractors verwenden die 3TDES-Algorithmen im CBC-Modus mit zufallsgeneriertem IV.

Plattformvirtualisierung – ESX-Modul

Das ESX-Modul verwendet für die Kommunikation mit Remote-VMware ESX-Knoten das TLS v1.0-Protokoll.

DTS

Die DTS-Programme verwenden durch die AES- oder 3TDES-Algorithmen zur Verfügung gestellte symmetrische Verschlüsselung mit unterschiedlichen Schlüssellängen, doch stets im CBC-Modus mit zufallsgenerierten IV.

CCS

CA ITCM kann CA Common Services verwenden, was optional installiert werden kann. Um eine detaillierte Beschreibung der FIPS-Compliance-Level des CA Common Services zu erhalten, überprüfen Sie "Appendix B FIPS 140-2 Encryption" im *CA NSM-Administrationshandbuch* , die im CA Bookshelf zur Verfügung stehen.

FIPS-Konformität von CA ITCM-externen Komponenten

Kryptographie hat in einem Computer neben den CA ITCM-Anwendungen eine Vielzahl von anderen Verwendungen.

Microsoft Windows-Betriebsumgebungen

Der Microsoft-Kryptographieanbieter Microsoft Enhanced Cryptographic Service Provider [RSAENH CSP] ist unter mehreren Windows-Betriebsumgebungen FIPS-140-zertifiziert. Eine Liste dieser FIPS-zertifizierten Betriebsumgebungen finden Sie unter http://technet.microsoft.com/en-us/library/cc750357.aspx. Unter dieser Verknüpfung wird auch beschrieben, wie die lokale Sicherheitsrichtlinie für die Verwendung von FIPS-konformer Kryptografie aktiviert werden kann. Um FIPS-Konformität zu erreichen, müssen Sie die lokale Sicherheitsrichtlinie (Systemkryptographie: "FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden") für ENC aktivieren.

Hinweis: Berücksichtigen Sie die Auswirkungen eines Betriebs im Nur-FIPS-Modus (d. h., mit ausschließlicher Genehmigung FIPS-konformer Verschlüsselung). Weitere Informationen finden Sie unter FIPS 140-2-Unterstützung (siehe Seite 80).

SQL Server

Microsoft SQL Server ist ab Version 2005 SP1 FIPS--konform. Weitere Informationen zur Konfiguration von SQL Server für einen Betrieb im FIPS-konformen Modus finden Sie im Eintrag 920955 der Microsoft-Wissensdatenbank: http://support.microsoft.com/kb/.

Andere Komponenten

CA ITCM ist eine Geschäftslösungs-Suite, die aus verschiedenen Anwendungen und Komponentenmodulen besteht. Als Softwarepaket verwendet CA ITCM auch Komponenten und Dienste aus anderen CA-Gruppen und von Drittanbietern. Sofern nicht anderweitig beschrieben, werden durch diese Komponenten und Dienste keine kryptographischen Funktionen direkt in CA ITCM implementiert oder offengelegt. Ihre Konformität mit FIPS 140-2-zetrifizierten kryptographischen Modulen ist infolgedessen nicht dokumentiert. Informieren Sie sich in der entsprechenden Dokumentation, sowie in Informationen zu FIPS 140-2.

Kryptographische Vorgänge innerhalb von Betriebssystemen fallen außerdem in den Zuständigkeitsbereich des BS-Anbieters. Informationen zu Support bezüglich 140-2 sowie allgemeiner Kriterien, einschließlich Konformitäts-Level und/oder erforderlichen Konfigurations-Supports, bietet Ihnen die entsprechende Dokumentation der Anbieter.

Hinweis: Den aktuellen Stand der mit CA ITCM gelieferten Komponenten finden Sie in der Kompatibilitätsmatrix.

Nicht genehmigte Verwendung von Sicherheitsfunktionen

In manchen Fällen verwendet CA ITCM Sicherheitsfunktionen, die nicht durch die FIPS 140-2-Veröffentlichung genehmigt sind. Dies hat keine Auswirkung auf den 'normalen' CA ITCM-Betrieb im -Nur-FIPS-Modus.

Asset Management-Agent – Software-Signatur-Scanner

Wenn eine Software-Signatur für ein <file>-Tag einen "md5"-Attributwert enthält, verwendet der Signature-Scanner eine private Implementierung des MD5-Codes. Der Scanner prüft den Agenten-Computer Datei MD5 auf Dateien, die mit dem "md5"-Attribut übereinstimmen, bevor er für die Signatur ein positives Ergebnis zurückgibt. MD5 wird im Software-Signatur-Scanner für keine kryptographischen Zwecke verwendet.

Installation

Während der Installation von CA ITCM können für die Installation von Zertifikaten und Schlüsseln PKCS#12-basierte Dateien verwendet werden. Diese Dateien werden unter Verwendung eines Schlüssels verschlüsselt, der durch eine kennwortbasierte Schlüsselableitungs-Funktion (PBKD-Funktion) wie z. B. PBKDF2 aus dem PKCS#5 v2.0-Standard abgeleitet wurde. Während der Installation werden diese Dateien extrahiert und durch nicht kennwortbasierte Techniken geschützt.

Hinweis: Wie im Abschnitt 7,1 des FIPS 140-2 Implementation Guidance-Dokuments dargestellt, ist kennwortbasierte Schlüsselableitung (kennwortbasierte Schlüsselerstellung) für asymmetrische Schlüsselvereinbarungen dezidiert verboten.

Terminologieglossar

Anwendung

Eine *Anwendung* ist eine Software, zum Beispiel Microsoft Word.

Anwendungsvirtualisierung

Anwendungsvirtualisierung ist die Verkapselung einer Anwendung, indem sie vom zu Grunde liegenden Betriebssystem abgetrennt wird, unter dem es ausgeführt wird. In der Laufzeit wird die Anwendung dazu gebracht, so zu handeln, als ob sie direkt mit dem ursprünglichen Betriebssystem und allen davon verwalteten Ressourcen verbunden ist, aber in Wirklichkeit ist es nicht so.

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) ist einer der SCAP-Standards. Er enthält Standard-IDs und ein Wörterbuch zu sicherheitsbezogenen Systemkonfigurationsproblemen. Eine Rollendefinition in einem SCAP-Datenstrom kann Referenzen zu einer oder mehreren CCE-IDs, enthalten, was angibt, dass die Regel eine spezifische CCE-Konfigurationsanweisung oder eine Konfigurationskontrolle darstellt. Weitere Informationen erhalten Sie unter http://cce.mitre.org/.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) ist einer der SCAP-Standards. Er enthält Standard-IDs und ein Wörterbuch zu Plattform- und Produktnamen. Einige Elemente in XCCDF-Dateien, zum Beispiel, können auf die Anwendung ausschließlich auf bestimmten Plattformen beschränkt werden, und die erfolgt mittels CPE-IDs. Weitere Informationen erhalten Sie unter http://cpe.mitre.org/.

Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) ist ein Wörterbuch gebräuchlicher Begriffe (CVE-Identifikatoren) für öffentlich bekannte Sicherheitslücken. Diese Identifikatoren erleichtern das Austauchen von Daten über mehrere Netzwerk-Sicherheitsdatenbanken und Hilfsprogramme hinweg. CVE ist nur eine der in SCAP verwendeten Komponenten. Weitere Informationen finden Sie unter http://cve.mitre.org/.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) ist einer der SCAP-Standards. Es enthält Standards für die Übermittlung und die Bewertung der Auswirklungen von Sicherheitslücken. Weitere Informationen erhalten Sie unter http://www.first.org/cvss/index.html.

Connectors

Connectors sind die Verknüpfungen von Produkten, die Connector-Daten für externe Produkte oder *Domänen-Manager* verarbeiten. Jeder Connector ruft Informationen seines Domänen-Managers ab und übermittelt die Informationen über das Connector-Framework an das Consumer-Produkt zur Anzeige und Analyse. Connectors können auch eingehende Vorgänge für Daten im Quell-Domänen-Manager veranlassen, beispielsweise Objekterstellung. Connectors verwenden ein vereinheitlichtes Connector-Framework, um die Integration mit mehreren Produkten zu ermöglichen, die Sie verwenden.

Desktop-Aktualisierung

Bei der *Desktop-Aktualisierung* wird der virtuelle Desktop in den Originalstatus zurückversetzt. Verknüpfte Klone verfolgen Änderungen für den virtuellen Rechner mit dem Klon nach. Um die Speicherzuweisungen mit dem Klon zu steuern, stellt VMware View den Aktualisierungsvorgang bereit, der den Klon auf die Baseline zurücksetzt und alle für Änderungsnachverfolgungen bereitgestellten Deltas freigibt. Demnach gehen alle auf dem Systemdatenträger seit der Erstellung des Klons oder seiner letzten Aktualisierung oder Neuzusammenstellung gespeicherten Informationen verloren. Im Gegensatz zur Desktop-Neuzusammenstellung wird dasselbe Golden Template wie vor dem Aktualisierungsvorgang verwendet.

Desktop-Neuzusammenstellung

Die *Desktop-Neuzusammenstellung* ist ein Prozess, bei dem dem virtuellen Desktop eine neues Golden Template zugewiesen wird. Betriebssysteme und Anwendungen müssen während ihrer Lebenszeit verwaltet werden, um Probleme mittels Hotfixes oder Services Packs zu beheben oder neue Funktionen durch neue Versionen bereitzustellen. Für verknüpfte Klone bedeutet dies, dass das Master-Image oder das Golden Template aktualisiert werden muss. Sobald die Aktualisierungen abgeschlossen sind, wird der verknüpfte Klon neu zusammengestellt und wird aktiv. Während der Operation der Neuzusammenstellung werden die entsprechenden verknüpften Klone mit dem neuen Golden Template verknüpft und aktualisiert.

Durch Staging bereitgestelltes Image der virtuellen Anwendung

Ein *zwischengespeichertes Image einer virtuellen Anwendung* ist das Image einer virtuellen Anwendung, das im File System eines Computers entdeckt wurde.

Eigenständige Umgebung

Als *eigenständige Umgebung* wird eine Umgebung bezeichnet, in der die Benutzer des Host- und des Viewer-Computers sämtliche Einstellungen, Eigenschaften und die Lizenzierung der CA ITCM-Remote Control-Komponente lokal verwalten. Eingerichtet wird sie mit Hilfe einer eigenständigen Agenten-Installation. Wenn Sie die Installation manuell ausführen möchten, muss das Setup für den RC-Agenten direkt aufgerufen werden.

Eigenständige virtuelle Anwendung

Eine *eigenständige virtuelle Anwendung* ist eine virtuelle Anwendung, die so zur Verfügung gestellt worden ist, dass das als Quelle verwendete Image der virtuellen Anwendung auf dem System beherbergt wird, auf dem es zur Verfügung gestellt worden ist.

eXtensible Configuration Checklist Description Format (XCCDF)

eXtensible Configuration Checklist Description Format (XCCDF) ist eine Spezifikationssprache, die zum Schreiben von Sicherheits-Checklisten, Benchmarks und ähnlichen Arten von Dokumenten verwendet wird. Ein XCCDF-Dokument stellt eine strukturierte Sammlung von Sicherheitskonfigurationsregeln für eine Gruppe von Zielcomputern dar. Die Spezifikation unterstützt den Austausch von Informationen, die Generierung von Dokumenten, die Anpassung an Organisationen und Situationen, die automatisierte Compliance-Kontrolle sowie die Bewertung der Compliance. Weitere Infos finden Sie unter http://nvd.nist.gov/xccdf.cfm.

Federal Information Processing Standard (FIPS)

Federal Information Processing Standard (FIPS) ist ein Sicherheitsstandard, der vom NIST herausgegeben und genehmigt wird. Es gibt an, welche Sicherheitsanforderungen von einem kryptographischen Modul erfüllt werden müssen, die innerhalb eines Sicherheitssystems verwendet werden, das vertrauliche, aber nicht geheime, Information schützt.

FIPS-bevorzugt

FIPS-bevorzugt ist eine Betriebsart für CA ITCM, in der Großteil der kryptographischen Operationen FIPS-kompatibel sind, wenige Verschlüsselungen werden im früheren Format belassen. In diesem Modus ist CA ITCM rückwärts-kompatibel mit den früheren Versionen von CA ITCM.

FIPS-kompatible Kryptographie

FIPS-kompatible Kryptographie bezieht sich auf die Verwendung von FIPS 140-2-zertifizierten Modulen, FIPS-anerkannt, und von FIPS zugelassene Verfahren und Algorithmen für Kryptographie.

FIPS-zertifiziertes Kryptographiemodul

FIPS-zertifiziertes Kryptographiemodul bezieht sich auf das Modul "RSA CryptoC BSAFE", das für FIPS 140-2zertifiziert ist.

Flüchtige Klone

Flüchtige Klone sind virtuelle Desktops aus dem flüchtigen Pool von VMware View-Benutzerdaten, die vorübergehend integriert sind. Sobald ein Benutzer sich abmeldet, wird der Klon aktualisiert, und alle Benutzerdaten auf dem Systemdatenträger gehen verloren.

Gast

Ein *Gast* in der Terminologie der generischen Plattformvirtualisierung ist der virtuelle Rechner und das Gastbetriebssystem.

Gastbetriebssystem

Das *Gastbetriebssystem* führt das Betriebssystem, das in einem virtuellen Rechner ausgeführt wird.

Gehostete virtuelle Umgebung

Eine *gehostete virtuelle Umgebung* ist die Virtualisierungs-Software, die zusätzlich zu einem Hostbetriebssystem, das heißt, dem physischen Rechner, dem Host-BS, und dem Hypervisor ausgeführt wird.

Gestreamte virtuelle Anwendung

Eine *gestreamte virtuelle Anwendung* ist eine virtuelle Anwendung, die derart zur Verfügung gestellt worden ist, dass das als Quelle verwendete Image der virtuellen Anwendung auf einem anderen Remote- System beherbergt wird, als dem System ist, in dem es zur Verfügung gestellt wird.

Gestreamtes Image der virtuellen Anwendung

Ein *gestreamtes Image der virtuellen Anwendung* ist das Image einer virtuellen Anwendung, das als über das Netzwerk für einen Computer verfügbar entdeckt wurde. Die Entdeckung des gestreamten Image einer virtuellen Anwendung wird üblicherweise nur möglich sein, wenn die virtuellen Anwendungen sich innerhalb des zur Verfügung gestellten Images befinden.

Golden Template

In der CA ITCM-Terminologie ist das *Golden Template* der virtuelle Rechner, von dem aus die virtuellen Desktops geklont werden.

Host

Ein *Host* in der Terminologie der generischen Plattformvirtualisierung ist der physische Rechner, das Host-Betriebssystem und der Hypervisor.

Host-Betriebssystem

Das *Hostbetriebssystem* ist das Betriebssystem, das auf einem physischen Rechner ausgeführt wird.

Host-Cluster

Der *Hostcluster* ist die Gesamtmenge der Datenverarbeitungs- und Speicherressourcen einer Gruppe von Hosts, die zum Teil oder insgesamt das gleiche Netzwerk und den gleichen Speicher gemeinsam nutzen.

Hypervisor

Der *Hypervisor* ist die Virtualisierungs-Softwareschicht, die physische Hardware im Namen des Gastbetriebssystems simuliert. Dieser Begriff ist synonym zu Virtual Machine Monitor (VMM).

Image der virtuellen Anwendung

Ein *Image der virtuellen Anwendung* enthält eine oder mehrere virtuelle Anwendungen, die in einer Datei gespeichert wurden, möglicherweise mit einem Set unterstützender Metadatendateien.

Image-Definition der virtuellen Anwendung

Eine *Image-Definition der virtuellen Anwendung* bezeichnet die "Spur" für die Entdeckung des Image einer virtuellen Anwendung. Um ein Bild zu entdecken, dass eine oder mehrere eingeschlossene virtuelle Anwendungen enthält (in ihm gespeichert), müssen normale Softwaresignaturen mit der Image-Definition der virtuellen Anwendung verknüpft werden.

Instanz-Softwarestatusdatenbank

Die *Instanz-Softwarestatusdatenbank* ist ein Bestandteil der Softwarestatusdatenbank, die den Verlauf sämtlicher durch den Agent ausgeführten Softwarejobs enthält, die auf einem Nicht-Golden-Template-System ausgeführt wurden, d. h. alle Klone des Golden Template.

Konfigurationsansicht

Eine *Konfigurationsansicht* ist eine angepasste Windows-Benutzeroberfläche, auf der Sie Konfigurationsrichtlinien für bestimmte Komponenten oder Funktionen bearbeiten können. In den Konfigurationsansichten werden die relevanten Richtlinien für eine Komponente oder für eine Funktion unabhängig davon aufgeführt, an welcher Stelle sie sich tatsächlich in der Hierarchie und in der DSM-Explorer-Baumstruktur befinden.

Master-vDisk

In Citrix XenDesktop ist eine *Master-vDisk* die initiale vDisk, die vom Golden Template-Computer generiert wird.

Masterzielgerät

In Citrix XenDesktop ist ein *Masterzielgerät* der Basis-Desktop mit dem BS und dem erforderlichen Satz an Anwendungen, von dem eine vDisk generiert wird.

MITRE

Die *MITRE Corporation* ist eine gemeinnützige Organisation, die für Tätigkeiten in öffentlichem Interesse gegründet wurde. MITRE bietet Übersetzungsprogramme, Quellcode, Schemata, und Dateien kostenlos an, damit Einzelpersonen und Organisationen auf sie bauen und sie erweitern können. Ovaldi ist ein solches frei erhältliches Übersetzungsprogramm

National Institute of Standards and Technology (NIST)

Das National Institute of Standards and Technology (NIST) ist ein nichtregulierendes Bundesamt des US-Handelsministeriums. Aufgabe des NIST ist es, die US-amerikanische Innovation und industrielle Wettbewerbsfähigkeit zu fördern, indem es die Wissenschaft, Standards und Technologie des Messens so fördert, dass die wirtschaftliche Sicherheit und unsere Lebensqualität verbessert werden. Die US-amerikanische nationale Datenbank für Sicherheitslücken, National Vulnerability Database (NVD), die vom NIST betrieben wird, bietet ein Repository und Daten-Feeds mit Inhalten, die SCAP-Standards verwenden. Es ist außerdem das Repository für einige offizielle Daten zu SCAP-Standards. So definiert NIST offene Standards innerhalb des SCAP-Kontextes und definiert die Zuordnungen zwischen den SCAP-Aufzählungsstandards.

Nicht verknüpfte Klone

In VMware View sind *nicht verknüpfte Klone* oder vollständige Klone vollständige Kopien des Master- oder Golden Images. Der Klon enthält eine Kopie des Images, und alle Änderungen am System bei Benutzersitzungen werden in dieser Kopie gespeichert.

Normale Anwendung

Eine *normale Anwendung* ist Anwendungssoftware, die nicht virtualisiert worden ist und die in traditioneller Weise installiert und ausgeführt werden kann. Wenn Versionen, Patches, und Suiten erwähnt werden, handelt es sich um normale Anwendungen.

Nur-FIPS

Nur-FIPS ist eine Betriebsart für CA ITCM, in der nur FIPS-kompatible Kryptographie erlaubt ist. In diesem Modus ist CA ITCM nicht rückwärtskompatibel mit den früheren Versionen von CA ITCM.

Offline-Patching

Mit dem Offline-Patching können Sie Patch-Inhalte und -Dateien remote exportieren und sie mit dem CA Patch Manager ohne Internetzugriff in der CA ITCM-Umgebung importieren.

Offline-RAC

Bei einem *Offline-RAC* handelt es sich um einen RAC-Task (Neuinstallation nach Absturz, Reinstall After Crash), der nicht durch den Manager, sondern durch den Agent gesteuert wird. Virtuelle Desktops werden häufig *erneut erstellt*, das heißt, wenn das Golden Template aktualisiert und die Festplatte zurückgesetzt wird, werden alle Änderungen am virtuellen Desktop seit der vorherigen Zurücksetzung effektiv ungültig gemacht. Bei virtuellen Desktops ist nicht der Manager, sondern der Agent für die Erstellung des RAC-Jobcontainers verantwortlich. Bei einer Datenträgerzurücksetzung initiiert der Agent einen Offline-RAC, um sämtliche Software wiederherzustellen, die für den Agent bereitgestellt wurde.

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) ist einer der SCAP-Standards. Es enthält Standard-XML für Testverfahren im Zusammenhang mit sicherheitsrelevanten Softwarefehlern, Konfigurationsproblemen und Patches sowie mit der Weitergabe der Testergebnisse. Alle Regelüberprüfungen in der Checkliste haben die Form von Referenzen zu OVAL-Definitionen, die in OVAL-Dateien aus dem SCAP-Datenstrom enthalten sind. Weitere Informationen erhalten Sie unter http://oval.mitre.org/.

Ovaldi

Ovaldi ist ein OVAL-Übersetzungsprogramm, das von der MITRE Corporation entwickelt wurde. Es ist eine frei verfügbare Referenzimplementierung, die erstellt wurde, um zu zeigen, wie Informationen von einem Computer zu Testzwecken erhalten werden können, um die OVAL-Definitionen für diese Plattform zu bewerten und auszuführen und um die Testergebnisse weiterzugeben. Das Übersetzungsprogramm zeigt die Nutzbarkeit der OVAL-Definitionen auf und sorgt für eine korrekte Syntax und die Einhaltung des OVAL-Schemas.

Paket mit eigenständiger virtueller Anwendung

Ein *Paket mit einer eigenständigen virtuellen Anwendung* ist ein Paket mit einer virtueller Anwendung, das verwendet wird, um eine virtuelle Anwendung in eigenständigem Modus zur Verfügung zu stellen.

Paket mit virtueller Anwendung (VAP)

Ein Image einer virtuellen Anwendung, das in ein oder mehr Software Delivery verpackt ist, wird als *virtuelles Anwenderpaket* bezeichnet. Diese Pakete werden verwendet, um virtuelle Anwendungen auf Computern zur Verfügung zu stellen.

Paket zum Streaming der virtuellen Anwendung

Ein *Paket zum Streaming der virtuellen Anwendung* ist ein Paket mit einer virtueller Anwendung, das verwendet wird, um eine virtuelle Anwendung im Streaming- Modus zur Verfügung zu stellen.

Paket zur Bereitstellung der virtuellen Anwendung durch Staging

Ein *Paket zur Bereitstellung der virtuellen Anwendung durch Staging* ist ein Paket mit einer virtuellen Anwendung, das verwendet wird, um das Image der virtuellen Anwendung durch Staging bereitzustellen.

Paketformat

Das *Paketformat* ist eine Eigenschaft eines Softwarepakets. Formate sind "normal" und "virtuell".

Pakettyp

Der *Pakettyp* ist eine Eigenschaft eines Softwarepakets. Derzeitige Typen sind Allgemein, MSI, SXP, PIF und PKG. Paket-Typ wird nicht verwendet oder geändert, um virtuelle Anwendungspakete zu unterstützen.

Partition

Eine *Partition* ist eine isolierte Instanz eines Hostbetriebssystems. Partitionen verwenden normalerweise keine Gastbetriebssysteme, weil sie alle das Betriebssystem des Hosts gemeinsam nutzen.

Partitionierte virtuelle Umgebung

Eine *partitionierte virtuelle Umgebung* ist eine Umgebung, in der mehrere Instanzen des Host-Betriebssystems isoliert auf dem gleichen physischen Rechner ausgeführt werden können. Streng genommen handelt es sich nicht um eine Virtualisierungs-Technologie, aber sie wird verwendet, um die gleichen Probleme zu lösen.

Permanente Klone

Permanente Klone sind virtuelle Desktops des permanenten Pools, die in ihrer Form bestehen bleiben, nachdem sich der Benutzer abgemeldet hat, bis sie aktualisiert oder erneut erstellt werden. VMware View bietet integrierte getrennte Geräte für System- und Benutzerdaten mit den permanenten Klonen. Auf dem Benutzerdatengerät gespeicherte Informationen bleiben von jeder Aktualisierung oder Neuzusammenstellung unberührt, während Änderungen am Systemdatenträger verloren gehen.

Plattformvirtualisierung

Plattformvirtualisierung ist die Verkapselung von Computern oder Betriebssystemen, indem ihre physischen Merkmale vor den Benutzern verborgen werden und die Datenverarbeitungsplattform in der Laufzeit nachgeahmt wird.

Replikation

Bei der *Replikation* handelt es sich um einen Engine-Task zum Ausführen der Datenreplikation vom Domänen-Manager zum Enterprise-Manager und umgekehrt.

Sandkasten

Ein Sandkasten ist die Laufzeitumgebung einer Anwendung, die die Anwendung vom Betriebssystem und den Ressourcen des Computers sowie von anderen Anwendungen auf dem Computer isoliert. Der Grad der Isolation wird üblicherweise festgelegt, um der Anwendung einen beschränkten Zugriff auf Ressourcen des Betriebssystems zu erlauben, z. B. auf den Ordner "Eigene Dateien" .

Scalability-Server

Ein *Scalability-Server* ist der zentrale Server, um eine geographische Skalierbarkeit für Management-Tasks zu ermöglichen. Es handelt sich um einen verteilten Prozess, der die primäre Schnittstelle des Agenten ist.

SCAP-Datenstrom

Ein SCAP-Datenstrom besteht aus Sicherheits-Checklisten in automatischen XML-Formaten, Aufzählungen zu Sicherheitslücken und Produktnamen sowie Zuordnungen zwischen den Aufzählungen. Ein SCAP-Datenstrom besteht aus den folgenden XML-Dateien:

- Eine XCCDF-Datei
- Eine oder mehrere OVAL-Dateien
- (Optional) Eine CPE-Wörterbuchdatei

Schemazuordnung

Eine *Schemazuordnung* ist eine Zuordnung der mit Datenobjekten wie Benutzern, Computern und Gruppen verknüpften Attributnamen, die in einem externen Verzeichnis verwendet werden, zu den Attributnamen, die von den entsprechenden CA ITCM-Objekten verwendet werden. Der feste Satz und der Standardsatz der DSM-Attributnamen werden zur Abfrage von Verzeichnissen und zur Formulierung komplexer Abfragen und Berichte verwendet.

Security Content Automation Protocol (SCAP)

Das *Security Content Automation Protocol (SCAP)*, "S Cap" ausgesprochen, ist eine Methodik für die Verwendung von Standards wie XCCDF, CCE, CVE, CVSS, CPE und OVAL für automatisches Sicherheitslückenmanagement und die Bewertung der Einhaltung von Richtlinien (z. B. FISMA-Compliance). Genauer betrachtet SCAP ist eine Suite ausgewählter offener Standards, die Softwarefehler, sicherheitsrelevante Konfigurationsprobleme und Produktnamen aufzählen, und die Maßsysteme, um das Vorkommen von Sicherheitslücken festzustellen sowie Mechanismen, die die Ergebnisse dieser Messungen einordnen, um die Auswirkungen der entdeckten Sicherheitsprobleme zu beurteilen, enthalten. SCAP definiert, wie diese Standards kombiniert werden. Die nationale Datenbank für Sicherheitslücken stellt ein Repository und Daten-Feeds mit Inhalten, die die SCAP-Standards verwenden, zur Verfügung. Weitere Infos finden Sie unter http://nvd.nist.gov/.

Softwaresignatur

Eine *Softwaresignatur* definiert die Attribute einer Softwareanwendung, z. B. den Dateinamen der Hauptprogrammdatei, andere dazugehörende Dateien, den Größenbereich, Versionsbereich sowie das Erstellungs- und Änderungsdatum der Software. Alle diese Attribute einer Softwaresignatur dienen zur eindeutigen Identifikation einer Anwendung. Softwaresignaturen in Asset Management werden als Softwaredefinitionen erstellt. Sie können Softwaredefinitionen für ein Produkt, eine Version, einen Patch, eine Suite, eine Suite-Komponente oder ein Image der virtuellen Anwendung erstellen. Standardmäßig enthält Asset Management vordefinierte Softwaresignaturen für die branchenweit am häufigsten verwendeten Softwareprogramme.

Softwaretyp

Der *Software-Typ* ist eine Eigenschaft einer Softwaredefinition. Derzeitige Typen schließen Suite, Produkt, Version, Patch, und Image der virtuellen Anwendung ein.

Standorterkennung

Mit der *Standorterkennung* kann der DSM-Agent auf einem Computer den Standort des Computers feststellen.

Systemeigene virtuelle Umgebung

Eine *systemeigene virtuelle Umgebung* ist die Virtualisierungs-Software, die direkt auf dem physischen Rechner ausgeführt wird oder die als Host-Betriebssystem handelt oder auftritt (oft minimal), das heißt, der Rechner und der Hypervisor. Ein synonymer Begriff ist "Bare Metal-Umgebung".

vDisk

In Citrix XenDesktop ist eine *vDisk* oder ein virtueller Datenträger prinzipiell eine Image-Datei mit dem BS und dem erforderlichen Satz an Anwendungen.

Verknüpfte Klone

In VMware View verweisen *verknüpfte Klone* eines Master- oder Golden Images nur auf das Master- oder Golden Image, aber sie enthalten es nicht. Änderungen, die bei Benutzersitzungen am System vorgenommen werden, werden nicht im Master-Image gespeichert, sie werden nur in Delta-Dateien mit dem Klon beibehalten.

virtuelle Anwendung (VA)

Eine *virtuelle Anwendung* ist Software, die virtualisiert worden ist.

Virtuelle Festplatte

Eine *virtuelle Festplatte* ist ein Set von Dateien, die ein Dateisystem bildet, das als physischer Datenträger im Gastbetriebssystem erscheint.

Virtuelle Version

Eine *virtuelle Version* ist das virtuelle Äquivalent zur normalen Version und hat die gleiche grundlegende Bedeutung. Der Begriff wird verwendet, wenn man über Software-Inventar für virtuelle Anwendungen berichtet (nicht Images der virtuellen Anwendung). Beachten Sie, dass eine zur Verfügung gestellte virtuelle Anwendung entweder ein durch Staging bereitgestelltes oder ein per Datenstrom übertragenes Image einer virtuellen Anwendung als Quelle verwenden kann. Die virtuellen Anwendungen, die im Images der virtuellen Anwendung enthalten sind können als durch Staging bereitgestellt, aber nicht zur Verfügung gestellt angesehen werden.

Virtueller Desktop flüchtig verknüpfter Klone

Ein *virtueller Desktop flüchtig verknüpfter Klone* ist ein virtueller Rechner, der bei jeder Benutzeranmeldung aktualisiert oder erneut erstellt wird, und zwar ohne Persistenz für benutzerdefinierte installierte Anwendungen, Personalisierung usw.

Virtueller Desktop permanent verknüpfter Klone

Ein *virtueller Desktop permanent verknüpfter Klone* ist ein virtueller Rechner, der für einen bestimmten Benutzer dediziert ist, und der Benutzer kann das Hinzufügen bestimmter Software anfordern, Einstellungen anpassen usw. Die benutzerdefinierte Umgebung des Benutzers wird bei jeder Anmeldung wiederhergestellt. Dies wird so beibehalten, bis der virtuelle Desktop aktualisiert oder erneut erstellt wird. Zu diesem Punkt gehen alle auf dem Systemdatenträger installierten Softwareprodukte verloren.

Virtueller Desktop permanenter, nicht verknüpfter Klone

Ein *virtueller Desktop permanenter, nicht verknüpfter Klone* ist ein virtueller Rechner, der für einen bestimmten Benutzer dediziert ist, und er wird dem Benutzer bei jeder Anmeldung mit den entsprechenden benutzerdefinierten installierten Anwendungen, Benutzereinstellungen, Daten usw. angezeigt.

Virtueller Patch

Ein *virtueller Patch* ist das virtuelle Äquivalent zu einem normalen Patch und hat die gleiche grundlegende Bedeutung. Der Begriff wird verwendet, wenn man über Software-Inventar für virtuelle Anwendungen berichtet (nicht Images der virtuellen Anwendung).

Virtueller Rechner (VM)

Ein *virtueller Rechner* ist eine isolierte virtualisierte Umgebung, die einen Computer simuliert. Der virtuelle Rechner schließt definitionsgemäß das Gastbetriebssystem nicht ein.

Virtuelles Image

A *virtuelles Image* ist eine Datei oder Set von Dateien, die die vollständige Definition eines virtuellen Rechners, einschließlich seiner Hardware-Spezifikationen und virtuellen Festplatten enthalten. Es ist die Darstellung des Host-Dateisystems eines Gastes. Ein virtuelles Image kann online oder offline sein, je nach dem Laufstatus des virtuellen Rechners, den es abbildet.

XCCDF-Profil

Ein *XCCDF-Profil* ist eine Richtlinie, die auf den Zielcomputer angewendet oder mit der Konfiguration des Zielcomputers verglichen wird. Die XCCDF-Datei für jeden SCAP-Datenstrom definiert eine Liste der unterstützten Profile. Die XCCDF-Datei muss mindestens ein XCCDF-Profil enthalten, das angibt, welche spezifischen Regeln für die Überprüfung eines bestimmten Systemtyps verwendet werden. Sie können unterschiedliche XCCDF-Profile für jede anwendbare Betriebsumgebung, in der das System implementiert werden kann, erstellen.

Zentral verwaltete Hostumgebung

Bei einer *zentral verwalteten Hostumgebung* ist entweder ein Enterprise-Manager oder ein Domänen-Manager von Remote Control für die Konfiguration der Hosts sowie für die Authentifizierung von Viewer-Verbindungen verantwortlich. Außerdem verwaltet dieser Server die Adressbücher, die die Benutzer zur Hostsuche verwenden.

Zentral verwaltete Umgebung

In einer *zentral verwalteten Umgebung* steuert der Remote Control-Domänen-Manager die Hosteinstellungen durch Computerrichtlinien, Elemente im globalen Adressbuch (GAB), Lizenzierung des Agenten auf der Domäne und Benutzerberechtigungen. Dies ist die Standardeinstellung für CA IT Client Manager.

Zur Verfügung gestellte Anwendung

Eine *zur Verfügung gestellte Anwendung* ist eine Anwendung (normal oder virtuell), die für die Ausführung auf einem Zielcomputer verfügbar gemacht worden ist. Die Anwendung muss nicht lokal "installiert werden", um sie als zur Verfügung gestellt zu behandeln.

Zustandsüberwachung

Mithilfe der *Zustandsüberwachung (Health Monitoring, HM)* können Sie Alarme konfigurieren, Grenzwerte festlegen und den Gesamtzustand der CA ITCM-Infrastruktur überwachen.